BAOU
Education for All

ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી

(ગુજરાત સરકાર દ્વારા સ્થાપિત)

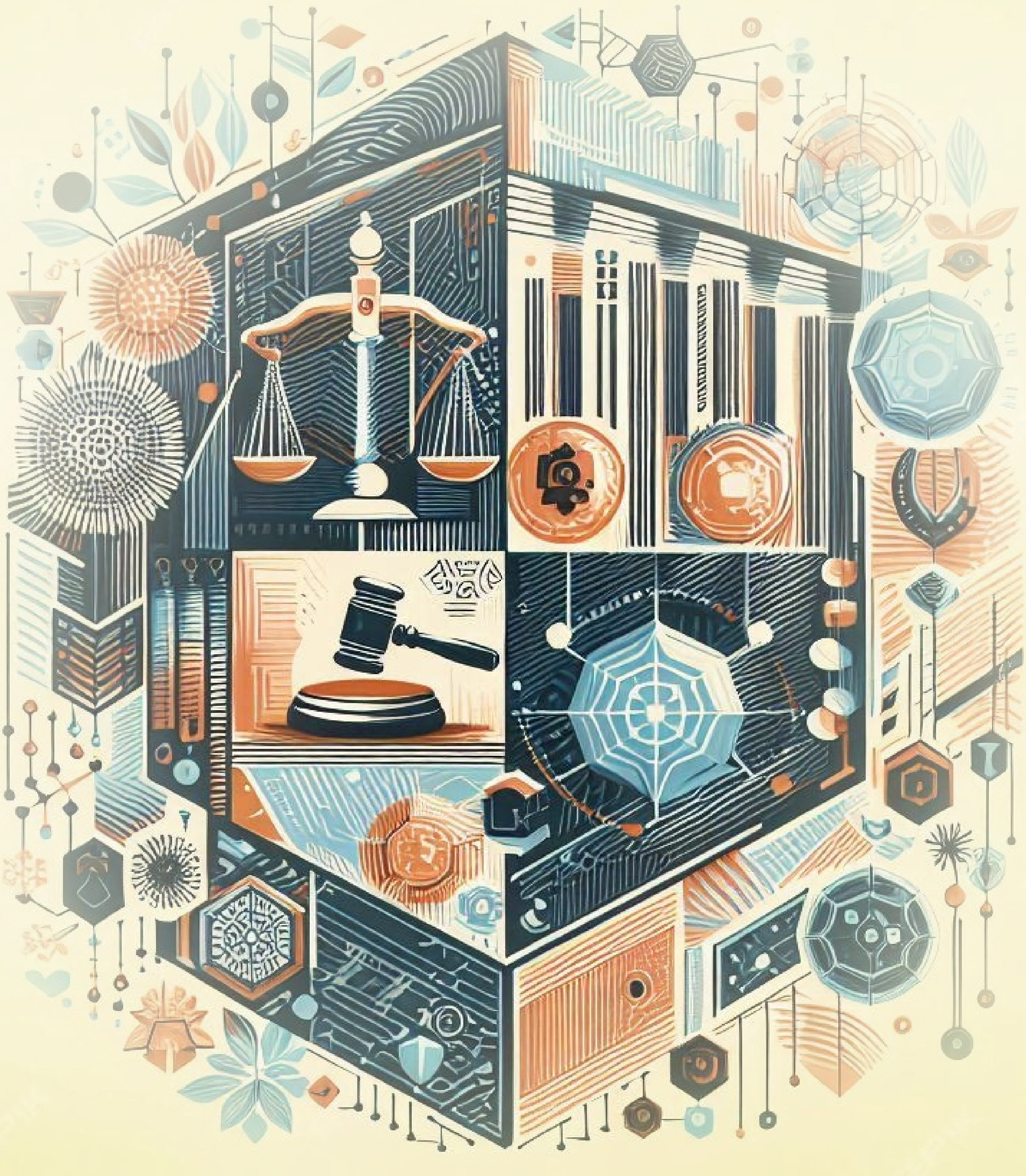
NAAC ACCREDITED A++ GRADE 3.55/4

ડિપ્લોમા - બૌદ્ધિક સંપત્તિ અને સાયબર અપરાધ
Diploma in Intellectual Property and Cybercrime (DIPACC)

સેમેસ્ટર – 2

પેપર - DIPACC - 8

સાયબર સુરક્ષા અને સાયબર અપરાધ સંબંધિત કાયદો
(Law relating to Cyber Security and Cyber Crime)



સ્વાધ્યાયનું અજવાળું

ભારતના સંવિધાનના સર્જક ભારતરત્ન ડૉ. બાબાસાહેબ આંબેડકરની પાવન સ્મૃતિમાં ગરવી ગુજરાતમાં ગુજરાત સરકારશ્રીએ ઈ.સ. 1994માં યુનિવર્સિટી ગ્રાન્ટ્સ કમિશન અને ડિસ્ટન્સ એજ્યુકેશન કાઉન્સિલની માન્યતા મેળવી અમદાવાદમાં ગુજરાતના એક માત્ર મુક્ત વિશ્વવિદ્યાલય ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટીની સ્થાપના કરી છે.

ડૉ. બાબાસાહેબ આંબેડકરની 125મી જન્મજયંતીના અવસરે જ ગુજરાત સરકાર દ્વારા યુનિવર્સિટી માટે અદ્યતન સગવડ સાથે, શાંત જગ્યા મેળવી, જ્યોતિર્મય પરિસરનું નિર્માણ કરી આપ્યું. BAOUના સત્તામંડળે પણ યુનિવર્સિટીના ઉજ્જવળ ભવિષ્ય માટે ખૂબ સહયોગ આપ્યો છે.

શિક્ષણ એટલે માનવમાં થતું મૂડીરોકાણ. શિક્ષણ લોકસમાજની ગુણવત્તા સુધારવામાં અધિક ફાળો આપી શકે છે. અહીં મને સ્વામી વિવેકાનંદનું શિક્ષણ વિષયક દર્શન યાદ આવે છે : 'જેનાથી ચારિત્ર્યઘડતર થાય, માનસિક ક્ષમતાનું નિર્માણ થાય, જેનાથી બૌદ્ધિક વિકાસ સાધી શકાય અને જેના થકી વ્યક્તિ પગભર બની શકે તેને શિક્ષણ કહેવાય.'

ડૉ.બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી શિક્ષણમાં આવા ઉમદા વિચારને વરેલી છે. તેથી વિદ્યાર્થીઓને ગુણવત્તાયુક્ત, વ્યવસાયલક્ષી, જીવનલક્ષી શિક્ષણની સગવડ ઘરે બેઠા મળી રહે એવા પ્રયત્નો મક્કમતા પૂર્વક કરે છે. સમાજના વિશાળ વર્ગને ઉચ્ચશિક્ષણ પ્રાપ્ત થાય, છેવાડાના માણસોને ઉત્તમ કેળવણી એમનાં રોજિંદાં કામો કરતાં પ્રાપ્ત થતી રહે. વ્યાવસાયિક લોકોને આગળ ભણતરની ઉત્તમ તક સાંપડે અને જીવનમાં પોતાની ક્ષમતાઓ, કૌશલ્યોને પ્રગટ કરી સારી કારકિર્દી ઘડે, સ્વાવલંબી બની ઉત્તમ જીવન જીવતાં સમાજ અને રાષ્ટ્રનિર્માણમાં પોતાનું પ્રદાન આપે એ માટે પ્રયાસરત છે.

'સ્વાધ્યાયઃ પરમં તપઃ' સૂત્રને ઓપન યુનિવર્સિટીએ કેન્દ્રમાં રાખીને અહીં પ્રવેશ મેળવતાં છાત્રોને સ્વઅધ્યયન માટે સરળતાથી સમજાય એવો ગુણવત્તાલક્ષી શૈક્ષણિક અભ્યાસક્રમ ઉપલબ્ધ કરાવી આપે છે. દરેક વિષયની પાયાની સમજણ મળે તેની કાળજી રાખવામાં આવે છે. વિદ્યાર્થીઓને રસ પડે અને રુચિ કેળવાય તેવાં પાઠ્યપુસ્તકો નિષ્ણાત અધ્યાપકો દ્વારા તૈયાર કરવામાં આવે છે. દૂરવર્તી શિક્ષણ પ્રાપ્ત કરવા ખેવના રાખતા કોઈ પણ ઉંમરના છાત્રોને માટે અભ્યાસસામગ્રી તૈયાર કરવા માટે શિક્ષણવિદો સાથે પરામર્શન કરવામાં આવે છે. એ પછી જ માળખૂ રચી, અભ્યાસસામગ્રી તૈયાર કરી પુસ્તક સ્વરૂપે છાત્રોનાં કરકમળોમાં આપે છે. જેનો ઉપયોગ કરીને વિદ્યાર્થી સંતોષપ્રદ અનુભવ કરી શકે છે.

યુનિવર્સિટીના તજ્જ્ઞ અધ્યાપકો ખૂબ કાળજીથી આ અભ્યાસક્રમોનું લેખન કરે છે. વિષયનિષ્ણાત પ્રોફેસરો દ્વારા એમનું પરામર્શન થાય પછી જ પરિણામલક્ષી અભ્યાસસામગ્રી યુનિવર્સિટીના વિદ્યાર્થીઓને પહોંચે છે. ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી જ્ઞાનનું કેન્દ્રબિંદુ બની રહી છે. વિદ્યાર્થીઓને 'સ્વાધ્યાય ટેલિવિઝન', 'સ્વાધ્યાય રેડિયો' જેવા દૂરવર્તી ઉપાદાનો થકી પણ એમના ઘર સુધી શિક્ષણ પહોંચાડવાનો પુરુષાર્થ થઈ રહ્યો છે. ઉમદા હેતુ, શ્રેષ્ઠ ધ્યેયને આંબવા પરિશ્રમરત યુનિવર્સિટીના જ્ઞાનની પરબમાં અધ્યાપકો તેમજ કર્મઠ કર્મચારીગણને અભિનંદન આપવા સાથે અમારી યુનિવર્સિટીના વિદ્યાર્થીઓ સફળ થવા ખૂબ મહેનત કરી, જીવન સફળ કરવાની સાથે જીવન સાર્થક કરે એવી પરમેશ્વરને પ્રાથના કરું છું.
અસ્તુ!

પ્રો. (ડૉ.) અમી ઉપાધ્યાય
કુલપતિ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી, જ્યોતિર્મય પરિસર, સરખેજ-ગાંધીનગર હાઈવે, છારોડી, અમદાવાદ

Diploma in Intellectual Property and Cybercrime (DIPACC)

DIPACC - Paper – 8 - સાયબર સુરક્ષા અને સાયબર અપરાધ સંબંધિત કાયદો

(Law relating to Cyber Security and Cyber Crime)

નિદર્શન

પ્રો. યોગેન્દ્ર પારેખ નિયામક, સ્કૂલ ઓફ હ્યુમેનિટીઝ એન્ડ સોશિયલ સાયન્સીસ, ડૉ.બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી અમદાવાદ

સંપાદક

ડૉ. ભાવેશ એચ. ભરાડ અધ્યક્ષ, ડિપાર્ટમેન્ટ ઓફ હ્યુમન રાઈટ્સ એન્ડ ડ્યુટીઝ, સ્કૂલ ઓફ લો, ગુજરાત યુનિવર્સિટી અમદાવાદ.

ડૉ. ભાગ્યશ્રી રાજપૂત DIPACC કોર્સ કો-ઓર્ડીનેટર અને આસિસ્ટન્ટ પ્રોફેસર, સમાજશાસ્ત્ર, સ્કૂલ ઓફ હ્યુમેનિટીઝ એન્ડ સોશિયલ સાયન્સીસ, ડૉ.બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી અમદાવાદ.

વિષય સમિતિ

ડૉ. ભાવેશ એચ. ભરાડ અધ્યક્ષ, ડિપાર્ટમેન્ટ ઓફ હ્યુમન રાઈટ્સ એન્ડ ડ્યુટીઝ, સ્કૂલ ઓફ લો, ગુજરાત યુનિવર્સિટી અમદાવાદ.

ડૉ. અરુંધતી દાસાણી આસિસ્ટન્ટ પ્રોફેસર, એ.એમ.પી સરકારી લો કોલેજ, યાજ્ઞિક રોડ, રાજકોટ

સુશ્રી સત્યા એસ. પોગારૂ પેટન્ટ એજન્ટ, પાર્ટનર અને વાઇસ-પ્રેસિડેન્ટ, એન્જીનિયર અને સોફ્ટવેર ગ્રુપ, લેક્સપર્ટ કોન્સિલિયમ એલએલપી, અમદાવાદ

લેખન

ડૉ. જશવંત આર. દવે આસિસ્ટન્ટ પ્રોફેસર, IT વિભાગ, વિશ્વકર્મા સરકારી ઈજનેરી કોલેજ, અમદાવાદ

શ્રી નિકુંજ સી. ગામિત આસિસ્ટન્ટ પ્રોફેસર, IT વિભાગ, વિશ્વકર્મા સરકારી ઈજનેરી કોલેજ, અમદાવાદ

સુશ્રી નૈમિષા એસ. ત્રિવેદી આસિસ્ટન્ટ પ્રોફેસર, IT વિભાગ, વિશ્વકર્મા સરકારી ઈજનેરી કોલેજ, અમદાવાદ

વિષય પરામર્શન

ડૉ. વિમલકુમાર પરમાર આચાર્ય, શ્રી કે. પી. શાહ લો કોલેજ, અરવિંદ માર્ગ, જામનગર

ભાષા પરામર્શન

પ્રિ. ઘનશ્યામ કે. ગઢવી નિવૃત્ત આચાર્ય, શ્રીમતી ચૌધરી સાર્વજનિક કૉલેજ, મહેસાણા

પ્રકાશક

કુલસચિવ, ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી, અમદાવાદ.

પ્રકાશન વર્ષ : **2025: પ્રથમ આવૃત્તિ**

ISBN NO: **978-93-5598-630-6**

978-93-5598-630-6

: સર્વાધિકાર સુરક્ષિત :

આ પાઠ્યપુસ્તક ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટીના ઉપક્રમે વિદ્યાર્થીલક્ષી સ્વઅધ્યયન હેતુથી દૂરવર્તી શિક્ષણના ઉદ્દેશને કેન્દ્રમાં રાખી તૈયાર કરવામાં આવેલ છે. જેના સર્વાધિકાર સુરક્ષિત છે. આ અભ્યાસસામગ્રીનો કોઈ પણ સ્વરૂપમાં ઉપયોગ કરતાં પહેલાં ડૉ.બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટીની લેખિત પરવાનગી લેવાની રહેશે.

ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી

(ગુજરાત સરકાર દ્વારા સ્થાપિત)

DIPACC – સેમેસ્ટર – 2

પાઠ્યક્રમ – 8 સાયબર સુરક્ષા અને સાયબર અપરાધ સંબંધિત કાયદો

(Law relating to Cyber Security and Cyber Crime)

એકમ-1

ઈ-કોમર્સ અને ઈ-કોન્ટ્રાક્ટ **01**

એકમ-2

ભારતમાં મોબાઈલ કાયદા **12**

એકમ-3

ઈન્ટરનેટ બેંકિંગ **21**

એકમ-4

નેટવર્ક સુરક્ષા **32**

એકમ-5

સોશિયલ મીડિયા અને સાયબર સુરક્ષા **51**

વિભાગીય પરિચય

વિદ્યાર્થીમિત્રો, સાયબર જગતમાં સુરક્ષાના મહત્વનો પરિચય આપવા, કાનૂની જાણકારીમાં વધારો કરવા, અને ડિજિટલ જગતમાં થતા ક્રાઈમોનો સામનો કેવી રીતે કરવો તેની સમજ આપવાના મુખ્ય ઉદ્દેશ્યથી DIPACC - Paper – 8 - સાયબર સુરક્ષા અને સાયબર ગુનાઓ સંબંધિત કાયદો (Law relating to Cyber Security and Cyber Crime) પાઠ્યક્રમનો સમાવેશ કરવામાં આવેલ છે. આ પાઠ્યક્રમ દ્વારા, ઈ-કોમર્સ, ઈ-કોન્ટ્રાક્ટ, ઈન્ટરનેટ બેન્કિંગ, અને નેટવર્ક સુરક્ષા જેવી મહત્વપૂર્ણ તકનીકી પ્રથાઓની વિસ્તૃત સમજણ મળશે. તે સાથે સાથે તેઓ સાયબર જગતમાં ગેરકાયદેસર પ્રવૃત્તિઓને અટકાવવા માટેના કાનૂની માવજત અને કાયદાકીય જોગવાઈઓની માહિતી મેળવી શકશે.

વિદ્યાર્થીમિત્રો, પ્રથમ એકમ ઈ-કોમર્સ અને ઈ-કોન્ટ્રાક્ટમાં, ઈ-કોમર્સ અને ઈ-કોન્ટ્રાક્ટના પાયાની સમજણ આપેલ છે. ઈ-કોન્ટ્રાક્ટની આવશ્યકતા, વિવિધ પ્રકારના ઈ-કોન્ટ્રાક્ટ તથા તેની સ્થિતિ, ઈ-કોન્ટ્રાક્ટના સંદર્ભમાં આંતરરાષ્ટ્રીય પરિસ્થિતિનું વર્ણન કરેલ છે.

બીજા એકમમાં ભારતમાં મોબાઈલ ઉપકરણોના વપરાશ સાથે સંકળાયેલા કાયદા અને નિયમો વિશે માર્ગદર્શન આપવામાં આવેલ છે. મોબાઈલ ડિવાઇસીસથી થતા સાયબર ગુનાઓ અને તેની સામે લડવા માટેના કાયદાકીય ઉપાયો વિશે માહિતી આપેલ છે.

ત્રીજા એકમમાં ઈન્ટરનેટ બેન્કિંગના માધ્યમથી થતા વિતરણ વ્યવહારો અને તેના પરિપ્રેક્ષ્યમાં સાયબર સુરક્ષા અને કાનૂની પડકારોની સમજણ આપવામાં આવી છે. ઈલેક્ટ્રોનિક બેન્કિંગ અને પેમેન્ટ સિસ્ટમ્સમાં સુરક્ષાના નિર્ણાયક પાસાઓ વિશે વિસ્તૃત માહિતીની ચર્ચા કરેલ છે.

ચોથા એકમમાં નેટવર્ક સુરક્ષાના મહત્વપૂર્ણ તત્વો અને તેનો સાયબર સુરક્ષા પરનો પ્રભાવ સમજાવવામાં આવ્યું છે. નેટવર્ક ઇન્ફ્રાસ્ટ્રક્ચરના સુરક્ષાત્મક ઉપાય અને તેનાથી જોડાયેલા કાનૂની જોગવાઈઓની સમજણ દર્શાવેલ છે.

વિદ્યાર્થીમિત્રો, પાંચમા એકમમાં સોશિયલ મીડિયા પ્લેટફોર્મ્સની બારીકીઓ અને તેનાથી સંકળાયેલા સાયબર ખતરાઓ અને કાયદાકીય પરિબળો વિશે માર્ગદર્શન આપવામાં આવ્યું છે. સોશિયલ મીડિયા પરનું સાયબર ગુનાઓ અને તેની સામે લડવા માટેના કાનૂની ઉપાયો પર ધ્યાન કેન્દ્રિત કરેલ છે.

એકમ-1 ઈ-કોમર્સ અને ઈ-કોન્ટ્રાક્ટ

: રૂપરેખા :

1.0 ઉદ્દેશ

1.1 પ્રસ્તાવના

1.2 ઈ-કોન્ટ્રાક્ટની આવશ્યકતા

1.3 ઈ-કોન્ટ્રાક્ટની પરિપૂર્ણતા માટેની આવશ્યકતાઓ

1.4 વિવિધ પ્રકારના ઈલેક્ટ્રોનિક કોન્ટ્રાક્ટ

1.5 ઈ-કોન્ટ્રાક્ટ સાથે સંબંધિત કાનૂની માળખું

1.6 ભારતમાં ઈ-કોન્ટ્રાક્ટની સ્થિતિ

1.7 ઈ-કોન્ટ્રાક્ટનાં સંદર્ભમાં આંતરરાષ્ટ્રીય પરિસ્થિતિ

● **સારાંશ**

1.8 તમારી પ્રગતિ ચકાસો

1.9 ચાવીરૂપ શબ્દો

1.10 સંદર્ભસૂચિ

1.0 ઉદ્દેશ

વિદ્યાર્થીમિત્રો, આ પ્રકરણનો અભ્યાસ કર્યા બાદ તમે;

- ઈ-કોન્ટ્રાક્ટ અને તેની જરૂરિયાત અંગેની સમજણ પ્રાપ્ત કરશો.
- ઈ-કોન્ટ્રાક્ટનાં પ્રકારો અને તેની પરિપૂર્તિ માટે જરૂરી પરિબળો અંગેની માહિતી મેળવશો.
- ભારત અને વિશ્વમાં ઈ-કોન્ટ્રાક્ટની સ્થિતિ અંગેનો ખ્યાલ પ્રાપ્ત કરશો.

1.1 પ્રસ્તાવના

કરાર કે કોન્ટ્રાક્ટ એટલે સરળ શબ્દોમાં કહીએ તો બે કે તે કરતાં વધારે વ્યક્તિઓ કે પક્ષકારો વચ્ચે કોઈ વસ્તુની ખરીદી/વેચાણ કે કોઈ સેવાના ઉપયોગ થતી સમજૂતી. આજના જમાનામાં કરાર (કોન્ટ્રાક્ટ) એ આપણા જીવનનો એક ભાગ થઇ ગયો છે. દુકાનમાંથી વસ્તુની ખરીદી કરવી, એક સ્થળેથી બીજા સ્થળે જવા માટે ટેક્ષી કરવી, આપણા ધંધાના વિકાસ માટે કોઈ બીજી કંપની સાથે જોડાણ કરવું આ બધું જ કરાર કે કોન્ટ્રાક્ટનાં જ ઉદાહરણ છે. ધ ઇન્ડિયન કોન્ટ્રાક્ટ ઍક્ટ (ભારતીય કરાર અધિનિયમ) 1872 અનુસાર માલ અથવા સેવાઓની ખરીદી/વેચાણ માટે બે અથવા વધુ પક્ષકારો વચ્ચે થતી સમજૂતીને કરાર કહેવામાં આવે છે. વૈશ્વિકીકરણ અને ટેક્નોલૉજીના પ્રસારને કારણે કાગળ ઉપર થતા કરારો હવે ઓનલાઈન કરારો (ઈ-કોન્ટ્રાક્ટ)માં પરિવર્તીત થઇ રહ્યા છે. ઈ-કોન્ટ્રેકટમાં તૈયાર કરવામાં આવતા દરેક દસ્તાવેજ ઓનલાઈન બનાવવામાં આવે છે અને ત્યારબાદ કરારમાં જોડાયેલ દરેક પક્ષકારો તે કરારને સમજી તેના ઉપર હસ્તાક્ષર પણ ઓનલાઈન જ કરે છે. આવી રીતે તૈયાર થતા દસ્તાવેજો અમલ કરવા યોગ્ય અને કાયદેસર રીતે બંધનકર્તા

દસ્તાવેજો છે જેનો ઉપયોગ સામાન્ય રીતે રોજગાર, ખરીદ/વેચાણ કે સેવાઓનાં આદાનપ્રદાન માટે થાય છે. ઓનલાઈન શોપિંગની વેબસાઈટ ઉપરથી કે ઓનલાઇન હરાજીમાં ભાગ લઈ કોઈ વસ્તુ ખરીદવી તથા પસંદગી પામેલા ઉમેદવારને નોકરી માટે ઓફર આપવી વગેરે ઈ-કોન્ટ્રેકટનાં ઉદાહરણ છે.

1.2 ઈ-કોન્ટ્રાક્ટની આવશ્યકતા

1.2.1. સમય અને ખર્ચનો બચાવ

આજે સમાજ જ્યારે ખૂબજ ઝડપથી આગળ વધી રહ્યો છે ત્યારે ધંધા અને રોજગારને સમાજની જરૂરિયાત મુજબ ઝડપી, યોગ્ય અને અસરકારક બનાવવા માટે ઈ-કોન્ટ્રાક્ટ ખૂબજ અગત્યના પૂરવાર થઇ રહ્યા છે. આપણે કલ્પના કરીએ કે ભારતની કોઈ એક સંસ્થાને વિદેશની કોઈ સંસ્થા સાથે ધંધા સંબંધિત કરાર કરવા છે. તો તેની પાસે પ્રથમ વિકલ્પ છે કે તે કરારની બે નકલ તૈયાર કરે, તેના ઉપર પોતાનાં હસ્તાક્ષર કરે અને કુરિયર દ્વારા તે વિદેશમાં રહેલી સંસ્થાને મોકલી આપે. તે સંસ્થા આ કરાર વાંચે અને યોગ્ય લાગે તો તેના ઉપર હસ્તાક્ષર કરી એક નકલ પોતાની પાસે રાખે અને અન્ય નકલ ભારતમાં આવેલી સંસ્થાને પાછી મોકલે. બીજો વિકલ્પ છે કે જેમાં બંને સંસ્થાના સક્ષમ હોદ્દેદારો કોઈ એક જગ્યાએ ભેગા થાય અને કરાર પર હસ્તાક્ષર કરે. ઉપરોક્ત પ્રથમ વિકલ્પમાં કુરિયરને કારણે સમયનો બિનજરૂરી વ્યય થશે જ્યારે બીજા વિકલ્પમાં બિનજરૂરી મુસાફરી ખર્ચ ભોગવવો પડશે પરંતુ જો આ બંને વિકલ્પોની જગ્યા એ ઈ-કોન્ટ્રાક્ટ તૈયાર કરે ઈ-મેઈલ કે અન્ય ઓનલાઈન માધ્યમનો ઉપયોગ કરી તે બીજા પક્ષકાર સુધી પહોંચાડી દેવામાં આવે તો સમય અને ખર્ચ બંને બચી શકે.

1.2.2. વિવિધ સોફ્ટવેરને કારણે કાર્યમાં સરળતા : વિશ્વમાં ઈ-કોન્ટ્રાક્ટની ઉપયોગીતા વધતા ઘણી કંપનીઓએ સરળતાથી ઈ-કોન્ટ્રાક્ટ થઇ શકે તે માટે વિવિધ સોફ્ટવેર તૈયાર કર્યા છે. જેમાં ઈ-કોન્ટ્રાક્ટ માટેના અલગ-અલગ પ્રકારના તૈયાર ટેમ્પ્લેટ આપેલા હોય છે. આ ટેમ્પલેટનાં ઉપયોગથી કોઈપણ વ્યક્તિ પોતાની જરૂરિયાત મુજબ ઈ-કોન્ટ્રાક્ટ ખૂબજ ઓછા સમયમાં તૈયાર કરી શકે છે.

1.2.3. બિનજરૂરી કાગળનો બચાવ : આપણે સૌ જાણીએ છીએ કે સમગ્ર વિશ્વમાં અત્યારે 'ગો ગ્રીન' નામની એક પહેલ ચાલી રહી છે જેના ભાગરૂપે શક્ય એટલો કાગળનો ઉપયોગ ઘટાળી વૃક્ષોને બચાવવાનો એક નમ્ર પ્રયાસ થઇ રહ્યો છે. આ અંતર્ગત જો ઈ-કોન્ટ્રાક્ટનો ઉપયોગ કરવામાં આવે તો બિનજરૂરી કાગળનો બચાવ થઇ શકે.

1.2.4. ઉન્નત સુરક્ષા પ્રદાન કરવા માટે : બે કે વધુ પક્ષકારો વચ્ચે થયેલ કરાર એક ગોપનીય દસ્તાવેજ છે જેનો ઉપયોગ માત્ર કંપનીના સક્ષમ હોદ્દેદારો જ કરી શકવા જોઈએ. કરારના આવા દસ્તાવેજો જો કબાટમાં રાખવામાં આવ્યા હોય તો શક્ય છે કે સક્ષમ હોદ્દેદારો સિવાય પણ બીજા આ દસ્તાવેજો સુધી પહોંચી શકે પરંતુ જો ઈ-કોન્ટ્રાક્ટ કરી આવા દસ્તાવેજોને ઈ-મેઈલ કે કોન્ટ્રાક્ટ મેનેજમેન્ટ સોફ્ટવેરમાં સાચવીને રાખેલા હોય તો માત્ર એવા લોકો જ કે જેમાંની પાસે ઈ-મેઈલ કે કોન્ટ્રાક્ટ મેનેજમેન્ટ સોફ્ટવેર વાપરવાની સત્તા છે તેઓ જ ઈ-કોન્ટ્રાક્ટનો ઉપયોગ કરી શકશે.

1.3 ઈ-કોન્ટ્રાક્ટની પરિપૂર્ણતા માટેની આવશ્યકતાઓ :

પક્ષકારો વચ્ચેનો કરાર કાયદેસર રીતે માન્ય તો જ છે જો તે કરાર સંબંધિત કાયદાની જરૂરિયાતોને સંતોષે, આજના સમયમાં ઇ-કોન્ટ્રાક્ટને પણ અન્ય કોઈપણ કરારની જેમ જ ગંભીરતાથી લેવામાં આવે છે તે માટે એવા આવશ્યક ઘટકો/સિદ્ધાંતો કે જે અન્ય કરારને

પૂરા કરવા માટે જરૂરી છે તે ઈ-કોન્ટ્રાક્ટ માટે પણ એટલા જ જરૂરી છે. આ ઘટકો/સિદ્ધાંતો નીચે મુજબ છે.

1.3.1. માન્ય પ્રસ્તાવ ઓફર (Offer) : ધ ઈન્ડિયન કોન્ટ્રાક્ટ ઍક્ટની કલમ 2(ક) મુજબ એક વ્યક્તિ કે પક્ષકારની બીજા કોઈ વ્યક્તિ કે પક્ષકાર સાથે કાયદેસર રીતે કરારમાં જોડાવાની ઈચ્છા અથવા અભિવ્યક્તિને પ્રસ્તાવ/ઓફર કહેવામાં આવે છે. ઈ-કોમર્સ વેબસાઈટ ઉપર કોઈ પણ વસ્તુ વેચવા માટે મૂકવામાં આવે છે તે પ્રસ્તાવ/ઓફર કહી શકાય નહીં કારણ કે તે કોઈ એક વ્યક્તિ કે પક્ષકાર માટે મૂકેલ નથી. તેને કરાર માટેનું આમંત્રણ કહી શકાય. જ્યારે ગ્રાહકો તે વસ્તુને પસંદ કરીને કાર્ટમાં મૂકે છે અથવા ઈ-મેલ દ્વારા અથવા વેબ પેજમાં બનેલ ઓનલાઈન ફોર્મ ભરીને પ્રતિસાદ આપે છે, ત્યારે તે ઓફરમાં પરિવર્તિત થાય છે. ધ ઈન્ડિયન કોન્ટ્રાક્ટ ઍક્ટની કલમ 5 મુજબ, પ્રસ્તાવ/ઓફર માટે પ્રદાન કરેલ સ્વીકૃતિનો સંદેશાવ્યવહાર (Communication) પૂર્ણ થાય તે પહેલાં ઓફરકર્તા કોઈપણ સમયે ઓફરને રદ કરી શકે છે.

1.3.2. કરારની સ્વીકૃતિ (Acceptance) : જ્યારે એક વ્યક્તિ કે પક્ષકારે આપેલી ઓફર બીજા કોઈ વ્યક્તિ કે પક્ષકાર સ્વીકારે અને તેની જાણ ઓફર કરનાર વ્યક્તિ કે પક્ષકારને કરે ત્યારે જ ત્યારે જ કરાર અસ્તિત્વમાં આવે છે. ઈ-કોન્ટ્રાક્ટમાં ઓફર અને ઓફરની સ્વીકૃતિ બંને વિવિધ ઓનલાઇન માધ્યમો જેમકે ઈ-મેઈલ, વેબસાઈટ પરના ફોર્મ અથવા તો કોન્ટ્રાક્ટ મેનેજમેન્ટ સોફ્ટવેર દ્વારા કરવામાં આવે છે.

1.3.3. ઓફર અને સ્વીકૃત રદબાતલ કરવાની સત્તા (Revocation of offer and Acceptance) : કરારમાં આપેલી સમય મર્યાદા પહેલા દરેક પક્ષકારોને ઑફર અને સ્વીકૃતિ રદ કરવાની સત્તા હોવી જોઈએ.

1.3.4. કરારની વિચારણા કાયદાને આધીન હોવી જોઈએ (Lawful Consideration) : ઈ-કોન્ટ્રાક્ટ માટેની વિચારણા કાયદાને અનુરૂપ હોવી જોઈએ. ધારોકે પક્ષકાર A પોતાના ઘરને પક્ષકાર B ને 10,000 રૂપિયામાં વેચવા તૈયાર થાય છે. અહીં, 10,000 રૂપિયાની રકમ ચૂકવવાનું પક્ષકાર Bનું વચન એ ઘર વેચવાના પક્ષકાર અના વચન માટે વિચારણા છે અને પક્ષકાર Aનું ઘર વેચવાનું વચન એ પક્ષકાર B ના 10,000 રૂપિયા ચૂકવવાના વચન માટે વિચારણા છે. આ કાયદેસર વિચારણાઓ છે.

1.3.5. જે ક્રિયા/વસ્તુ માટે કરાર થયો છે તે કાયદાકીય રીતે માન્ય હોવી જોઈએ (Lawful Object) : પક્ષકારો વચ્ચે જે કરાર થાય તેનો હેતુ કાયદેસર હોવો જોઈએ. એવા કરારો કે ..

- જે કાયદા દ્વારા પ્રતિબંધિત છે
- જેની પરવાનગી આપવામાં આવે, તો તે કોઈ બીજા કાયદાની જોગવાઈઓને નાબૂદ કરે
- જે કપટપૂર્ણ છે.
- જે કોઈ વ્યક્તિ અથવા મિલકતને ઈજા કરે છે
- જે જાહેર નીતિનું ઉલ્લંઘન કરે છે

તેને અદાલતો ગેરકાયદેસર ગણશે અને આવા કરારોને રદબાતલ ગણવામાં આવે છે. ઉદાહરણ તરીકે, માદક દ્રવ્યોનું વેચાણ માટેનો કરાર અથવા કોઈ વ્યક્તિનાં ઘરને બાળી નાખવા માટેનો કરાર વગેરે સખત પ્રતિબંધિત છે અને તેને કરાર માટેની માન્ય વિચારણા તરીકે ગણી શકાય નહીં.

1.3. 6. પક્ષકારો કરાર કરવા માટે સક્ષમ હોવા જોઈએ(Competent Parties) : કરાર કરનાર પક્ષકારો વ્યક્તિઓ હોવા જોઈએ અને તે વ્યક્તિઓ કાનૂની રીતે યોગ્ય અને સક્ષમ હોવા જોઈએ. પક્ષકાર માનસિક રીતે અસ્થિર કે 18 વર્ષથી નાનો ન હોવો જોઈએ. ઈ-કોન્ટ્રાક્ટ ભલે ઓનલાઈન માધ્યમથી ઈલેક્ટ્રોનિક ઉપકરણોની મદદથી થતા હોય પરંતુ કોઈપણ સંજોગોમાં આ ઈલેક્ટ્રોનિક ઉપકરણો જેવા કે કમ્પ્યૂટર, મોબાઈલ, લેપટોપ, ટેબ્લેટ વગેરે કરારના પક્ષકારો બનવા માટે સક્ષમ નથી.

1.3.7. સંમતિની યોગ્યતા (Free Consent) : સંમતિ જ્યારે બળજબરી, ખોટી રજૂઆત, અયોગ્ય પ્રભાવ, ભૂલ અથવા છેતરપિંડીથી થતી ન હોય ત્યારે તેને યોગ્ય સંમતિ કહેવામાં આવે છે.

1.3.8. શરતોની નિશ્ચિતતા (Certainty of Terms) : બંને પક્ષો કે જેમની વચ્ચે કરાર થઈ રહ્યો છે તેમની વચ્ચે નિયમો અને શરતોની નિશ્ચિતતા હોવી જોઈએ. ઈ-કોન્ટ્રાક્ટનાં કિસ્સામાં ઘણીવાર ઓફર આપનાર અને ઓફર સ્વીકારનાર વચ્ચે કરારની શરતોને અંતિમ ઓપ આપવા માટે ઘણીબધી વખત વાટાઘાટો વિવિધ ઓનલાઈન માધ્યમોની મદદથી થતી હોય છે. આ પરિસ્થિતિમાં કઈ શરતોને અંતિમ ગણાવી તે એક પડકાર સમાન પરિસ્થિતિ છે.

1.4 વિવિધ પ્રકારના ઈલેક્ટ્રોનિક કોન્ટ્રાક્ટ

1.4. 1. શ્રીંક-રૅપ કોન્ટ્રાક્ટ (Shrink Wrop Contract) : શ્રીંક-રૅપ કરારો મોટે ભાગે કમ્પ્યૂટર સોફ્ટવેર સાથે સંબંધિત છે. સોટવેરના બોક્ષને પેક કરવા માટે જે પ્લાસ્ટિકનું પેકેજીંગ કરવામાં આવે છે તેને શ્રીંક-રૅપ કહેવાય છે. જ્યારે વપરાશકર્તા તે પેકિંગને દૂર કરે છે ત્યારે તે એક કરારમાં પ્રવેશ કરે છે. સરળ શબ્દોમાં કહીએ તો, શ્રીંક-રૅપ કરાર એ એક પ્રકારનો લાયસન્સ કરાર છે જેમાં વસ્તુ સાથે કેટલાક નિયમો અને શરતો પણ પેકિંગમાં આવેલ હોય છે. ગ્રાહક જ્યારે પેકિંગ તોડીને વસ્તુનો ઉપયોગ કરે છે ત્યારે તે આપોઆપ જ કરારની સંમતિ આપે છે. નીચે આપેલા નિયમો અને શરતો છે જે શ્રીંક-રૅપ કરાર દ્વારા કરી શકાય છે.

- લાયસન્સ
- ફી અને પૈસાનું ભુકતાન
- વોરંટી
- જવાબદારીની મર્યાદાઓ

1.4.2. ક્લિક-રૅપ કોન્ટ્રાક્ટ (Click Wrap Contract) : મોટાભાગે જ્યારે આપણે કોઈ સોફ્ટવેરનું ઈંસ્ટોલેશન કરતા હોઈએ છીએ ત્યારે શરૂઆતમાં જ ઘણીબધી શરતો લખેલી આવે છે અને ત્યાં નીચે હું સંમત છું'' (I Agree) લખેલું ચેકબોક્ષ આવે છે. જો આપણે ખરેખર સોફ્ટવેર ઇન્સ્ટોલ કરવું હશે તો આપણે તે ''હું સંમત છું'' (I Agree) લખેલા ચેકબોક્ષમાં ક્લિક કરવી જ પડશે અને આપણે સૌ મોટાભાગે કોઈપણ શરતો વાંચ્યા વગર ત્યાં ક્લિક કરી પણ દઈએ છીએ. આ એક ક્લિક-રૅપ પ્રકારનો કોન્ટ્રાક્ટ છે.

ક્લિક-રૅપ કરારો સામાન્ય રીતે તે પ્રકારના કરારો અથવા લખાણના લાંબા બ્લોક્સ તરીકે ઓળખવામાં આવે છે જેને મોટાભાગે કોઈ વાંચતું નથી, આ બ્લોકસમાં કરારના નિયમો અને શરતો હોય છે. પરંતુ ઘણી વખત એવું બને છે કે આપણે ફક્ત 'હું સંમત છું' પર ક્લિક કરીએ છીએ અને કાર્યને આગળ વધારીયે છીએ. 'હું સંમત છું', બટન પર જ્યારે આપણે ક્લિક કરીએ છીએ, તેનો અર્થ એ છે કે અમે કરારના તમામ લેખિત

નિયમો અને શરતો સ્વીકારી લીધી છે. આવા પ્રકારના કરારોમાં બંને પક્ષો વચ્ચે વાટાઘાટની સંભાવના ખૂબ જ ઓછી હોય છે અને જો વપરાશકર્તા ખરેખર તે સોફ્ટવેર અથવા આ કરારથી સંબંધિત કોઈપણ અન્ય વસ્તુનો ઉપયોગ કરવા માંગતો હોય તો તેણે આ સ્વીકારવું જ પડે છે.

"હું સંમત છું" બટન પર ક્લિક કરવાની આ ક્રિયા ખૂબ સરળ દેખાય છે પરંતુ તે આપણને ગંભીર મુશ્કેલીમાં મૂકી શકે છે કારણ કે તે કાયદેસર રીતે લાગુ પાડી શકાય તેવા માન્ય કરારને જન્મ આપે છે. સેવાઓની શરતો, ગોપનીયતા નીતિઓ, કૉપીરાઇટ નીતિઓ અને બિન–જાહેરાત નીતિઓ માટે સામાન્ય રીતે ક્લિક-રૅપ કરારનો ઉપયોગ થાય છે.

ક્લિક-રૅપ કરારની વિશેષતાઓ

- આ કરારમાં આગળ વધવા માટે તમારે "હું સંમત છું" (I Agree) ઉપર ક્લિક કરવું જ પડે છે.
- આ પ્રકારના કરારમાં, સ્વીકૃતિ ખૂબ જ સ્પષ્ટ છે કારણ કે વપરાશકર્તા કાં તો ઓફર સ્વીકારશે અથવા નકારશે.
- સ્ક્રીન પર, વપરાશકર્તાને જાણ કરવી જોઈએ કે આ એક અમલ કરી શકાય તેવો કરાર છે અને તેની ક્રિયા માટે તેના પર બંધનકર્તા છે.
- કરારના નિયમો અને શરતો પર્યાપ્ત દૃશ્યતા સાથે વાંચી શકાય તેવા ફોન્ટમાં હોવી જોઈએ.
- કરારના તમામ નિયમો અને શરતો ભારતીય કરાર અધિનિયમ, 1872ની કલમ 10 સાથે સુસંગત રહેશે.
- વપરાશકર્તા દ્વારા આપવામાં આવતી માહિતી સામાન્ય રીતે ગ્રાહક દ્વારા ભવિષ્યમાં કોઈપણ વિવાદ અથવા મુકદ્દમાને ટાળવા માટે જાળવી રાખવામાં આવે છે.

1.4.3. બ્રાઉઝ–રૅપ કરારો(Brows Wrap Contract): વેબસાઇટ્સ પર કંઈપણ શોધતી વખતે અથવા વાંચતી વખતે બ્રાઉઝ–રૅપ કરારો કદાચ ઘણી વેબસાઇટ્સ પર જોવા મળે છે. તે એક પ્રકારના પોપ–અપ્સ તરીકે આવે છે જે તમને 'ઓકે' અથવા "હું સંમત છું" પર ક્લિક કરવાનું કહે છે, તેમ છતાં, તમે ત્યાં ક્લિક કરીને અથવા ક્લિક કર્યા વિના પણ વેબસાઇટનો ઉપયોગ કરી શકો છો. આ કરારમાં, ઘણીવાર વેબસાઇટની સ્ક્રીન પર નિયમો અને શરતો ધરાવતી હાઇપરલિંક અથવા વેબપેજ હોય છે. જ્યારે વ્યક્તિ ઉપરોક્ત નિયમો અને શરતો સાથે સંમત થાય છે, ત્યારે તે ઉપલબ્ધ માહિતીને વાપરી શકે છે અને તેમાં ઉપલબ્ધ ફાઈલ ડાઉનલોડ કરી શકે છે.

આજના સમયમાં વેબસાઈટમાં આપણે શું વાંચીએ, જોઈએ અને શોધીએ છીએ તેનો રેકોર્ડ રાખવા માટે વેબસાઈટ કુકીઝ રાખતી હોય છે. વપરાશકર્તા પાસેથી કુકીઝ રાખવા માટેની સંમતિ પણ પોપ–અપ્સ બતાવીને લેવામાં આવે છે જે પણ એક બ્રાઉઝ–રૅપ કરાર છે.

બ્રાઉઝ-રૅપ કરારની કાયદેસરતા બહુ સ્પષ્ટ નથી કારણ કે ક્લિક-રૅપ કરારથી વિપરીત, આ પ્રકારનો કરાર વપરાશકર્તા પાસેથી કોઈ સ્પષ્ટ સંમતિ માંગતો નથી. તેથી, કોર્ટે ધારે છે કે આ પ્રકારનો કરાર ગ્રાહક સામે બંધનકર્તા અથવા અમલપાત્ર નથી.

1.4.4. ઈ-મેઈલ કરાર (E-mail Contract) : કોઈપણ પ્રકારનો કરાર જ્યાં ઈ-મેઈલની મદદથી ઓફર અને સ્વીકૃતિની ચર્ચા કરવામાં આવે છે તેને ઈ-મેઈલ કોન્ટ્રાક્ટ કહેવામાં

આવે છે. ઈ-મેઈલ પર ઈલેક્ટ્રોનિક રીતે પણ હસ્તાક્ષર કરી શકાય છે, જે સમજૂતી ક્યારે કરાર બને છે તે નક્કી કરવા માટે એક મહત્ત્વપૂર્ણ માપદંડ છે.

1.4.5. ઈલેક્ટ્રોનિક હસ્તાક્ષરો (Electronic Signature): ઈલેક્ટ્રોનિક હસ્તાક્ષરો નિયમિત રીતે થતા હસ્તાક્ષરોનું એક ડિજિટલ અને ચકાસી શકાય તેવું સ્વરૂપ છે. ઈલેક્ટ્રોનિક હસ્તાક્ષરનો ઉપયોગ દસ્તાવેજો પર ઓનલાઈન હસ્તાક્ષર કરવા માટે થાય છે, જે સામાન્ય રીતે નીચે જણાવેલ બે રીતે થઈ શકે છે.

- OTPનો ઉપયોગ કરીને આધાર–આધારિત હસ્તાક્ષર
- ડિજિટલ હસ્તાક્ષર જે ક્રિપ્ટોગ્રાફી અને હેશ અલ્ગોરિધમ્સનો ઉપયોગ કરે છે અને વપરાશકર્તાઓને પાસવર્ડની મદદથી દસ્તાવેજો પર સહી કરવાની મંજૂરી આપે છે.

ઈલેક્ટ્રોનિક હસ્તાક્ષરને આઈટી ઍક્ટ, 2000 દ્વારા માન્યતા આપવામાં આવી છે, જેમાં ઈલેક્ટ્રોનિક હસ્તાક્ષરનો ઉપયોગ કરીને હસ્તાક્ષર કરાયેલ દસ્તાવેજોની કાનૂની માન્યતા અને અમલીકરણની ખાતરી કરવાની જોગવાઈઓ છે. તેથી ભારતીય કરાર કાયદામાં નિર્ધારિત માપદંડોને અનુરૂપ થયેલ કોઈપણ કરાર ઉપર ઈલેક્ટ્રોનિક હસ્તાક્ષરનો ઉપયોગ કરીને ઓનલાઈન હસ્તાક્ષર કરવામાં આવે છે તે ભારતમાં માન્ય ઈલેક્ટ્રોનિક કરાર છે.

1.4. 6. ઈ-કોમર્સ કરાર(E-commerce Contract): વેબસાઈટ પરથી ઓનલાઈન ખરીદી કે વેચાણ કરવા માટે ઉપયોગમાં લેવાતા ડિજિટલ કોન્ટ્રાક્ટને ઈ-કોમર્સ કોન્ટ્રાક્ટ અથવા ઓનલાઈન શોપિંગ કોન્ટ્રાક્ટ કહેવામાં આવે છે. એમેઝોન જેવી ઈ-કોમર્સ વેબસાઈટ પરથી વસ્તુ ખરીદવું એ ઈ-કોમર્સ કોન્ટ્રાક્ટ છે.

1.5 ઈ-કરાર સંબંધિત કાનૂની માળખું

ભારત અને સમગ્ર વિશ્વમાં ઈ-કોન્ટ્રાક્ટના વિસ્તરતા મહત્વ અને મૂલ્ય સાથે, વિવિધ પક્ષો ઈ-કોન્ટ્રાક્ટની કાનૂની જટિલતાઓને સતત શોધી રહ્યા છે અને તેનું મૂલ્યાંકન કરી રહ્યા છે. ભારતમાં હજુ પણ ખાસ કરીને ઈ-કોન્ટ્રાક્ટ સંબંધિત કોઈ કાયદા અને નિયમો નથી. જો કે, તેઓ ભારતમાં પ્રવર્તમાન વિવિધ કાયદાઓ દ્વારા નિયંત્રિત થાય છે. જે કાયદાઓ નીચે મુજબ છે.

1.5. 1. ભારતીય કરાર અધિનિયમ, 1872: ભારતીય કરાર અધિનિયમ, 1872 ભારતમાં કરારની રચના અને અમલીકરણની રીતને નિયંત્રિત કરે છે, તેથી જે કરાર કરવામાં આવે છે તે કાયદાકીય રીતે લાગુ કરવા માટે સંબંધિત અધિનિયમની કલમોને પૂર્ણ કરે છે. ભારતીય કરાર અધિનિયમની જોગવાઈઓ સામાન્ય કરારની જેમ જ ઈ-કોન્ટ્રાક્ટને પણ આવરી લે છે. કરાર કરવા માટે કોઈ પણ સંજોગોમાં જો ઈ-લેક્ટ્રોનિક માધ્યમનો ઉપયોગ કરવામાં આવે તો તે કરાર પણ કાયદેસર અને અમલપાત્ર ગણાશે કારણ કે કરાર સંબંધિત માહિતી ઈલેક્ટ્રોનિક માધ્યમ દ્વારા મોકલવામાં આવી હતી તે હકીકતને ધ્યાનમાં લીધા વિના, પક્ષકારો દ્વારા થતો કરારનો પ્રસ્તાવ અને તેનો સ્વીકાર મહત્ત્વપૂર્ણ છે અને તે કરારને લાગુ કરવા યોગ્ય છે.

1.5.2. ઈન્ફોર્મેશન ટૅક્નોલૉજી ઍક્ટ 2000 : ભારતીય કરાર અધિનિયમમાં કોન્ટ્રાક્ટ વિશે વાત કરવામાં આવી હોવા છતાં, તેણે ક્યારેય ઈ-કોન્ટ્રાક્ટની કાયદેસરતાનો ઉલ્લેખ કર્યો નથી. તેથી આઈટી ઍક્ટ, 2000માં ઈલેક્ટ્રોનિક માધ્યમ દ્વારા થતા વ્યવહારો અને સોદાઓને કાનૂની માન્યતા આપવાની જોગવાઈ કરવામાં આવે છે. IT ઍક્ટ, 2000 ની કલમ 3 અનુસાર, ઈલેક્ટ્રોનિક કોન્ટ્રાક્ટની ચકાસણી બંને પક્ષો દ્વારા કરાર પર ઈલેક્ટ્રોનિક હસ્તાક્ષર

કરીને અથવા અન્ય માન્ય ઈલેક્ટ્રોનિક પદ્ધતિ દ્વારા કરવામાં આવે છે. આવી રીતે કરેલા કરાર ભારતના કાયદા મુજબ માન્ય ગણવામાં આવે છે.

કોઈપણ કરાર જે ઈલેક્ટ્રોનિક રીતે થાય છે તેને આઈટી ઍક્ટ, 2000ની કલમ 10(ક) હેઠળ લાગુ કરવા યોગ્ય માનવામાં આવે છે. પાવર ઓફ એટર્ની, ટ્રસ્ટ ડીડ, વારસાઈ અને સ્થાવર મિલકત ખરીદવા અથવા ખસેડવા માટે ઉપલબ્ધ કરાર વગેરે કરારોનો આ કાયદા અંતર્ગત સમાવેશ થતો નથી. વધુમાં આ કાયદામાં સાયબર અપરાધ સંબંધિત વિવિધ કલમોમાં જુદી જુદી સજાનો પણ ઉલ્લેખ કરે છે.

1.5.3. ભારતીય પુરાવા અધિનિયમ, 1872 : હાલમાં, અદ્યતન વૉઇસ નોટ માટેના રેકોર્ડિંગ સાધનો, કમ્પ્યૂટરાઈઝડ કેમેરા, અદ્યતન કેમકોર્ડર અને વિડિયો કોન્ફરન્સ વગેરેને માન્ય પુરાવાની યાદીમાં ઉમેરવામાં આવી રહ્યા છે. સંબંધિત અધિનિયમના જુદા જુદા વિભાગોની મદદથી, આપણે ઈ-કોન્ટ્રાક્ટમાં સમાવિષ્ટ અલગ-અલગ પુરાવાની સ્થિતિ જાણી શકીએ છીએ.

1.5.4. પેમેન્ટ એન્ડ સેટલમેન્ટ ઍક્ટ, 2007 : વધતી જતી ટૅક્નોલૉજી સાથે, ઓનલાઈન પેમેન્ટની ઉપલબ્ધતાને કારણે પોતાની સાથે રોકડ રાખવાની જરૂરિયાત ઘટી રહી છે અને સૌ પોતાના નાણાકીય વ્યવહારો ઓનલાઈન પેમેન્ટની મદદથી કરી રહ્યા છે. આ પરિસ્થિતિમાં ઓનલાઈન થતા નાણાંકીય વ્યવહારોનાં નિયમન માટે એક કાયદેસર રચનાની જરૂર હતી જે પેમેન્ટ એન્ડ સેટલમેન્ટ ઍક્ટ, 2007 નાં સ્વરૂપે રજૂ કરવામાં આવેલ છે. આ માળખાને વધુ મજબૂત કરવા 2008માં પેમેન્ટ એન્ડ સેટલમેન્ટ ઍક્ટ, 2007ની જેમ જ પેમેન્ટ એન્ડ સેટલમેન્ટ સિસ્ટમ રેગ્યુલેશન્સ, 2008 ને લાગુ કરવામાં આવ્યો.

1.5.5. ઈલેક્ટ્રોનિક કોમર્સ ઍક્ટ, 1998 : ટૅક્નોલૉજીમાં કેટલાક સર્જનાત્મક ફેરફારો થવાના કારણે, ભારત સરકાર રાષ્ટ્રના વર્તમાન કાયદાઓમાં કેટલાક મહત્ત્વપૂર્ણ ફેરફારો પર વિચાર કરે અને તેને લોકહિતમાં પસાર કરે તેવી અપેક્ષા રાખવામાં આવી હતી. પરંતુ, ન્યાયમૂર્તિ અબુ ફઝલ તથા તેમનાં સહયોગીઓ એ ભારતીય કરાર અધિનિયમ, 1872ના હાલના હુકમમાં ફેરફારને સમર્થન આપવાનો ઈનકાર કર્યો હતો જેથી વર્તમાન પરિસ્થિતિ પ્રમાણે એક નવીન કાયદો બની શકે. આ અંતર્ગત ભારત સરકાર દ્વારા ઈન્ટરનેટ તથા ઈ-કોન્ટ્રાક્ટનાં અલગ અલગ પડકારોને ધ્યાનમાં રાખી ઈલેક્ટ્રોનિક કોમર્સ ઍક્ટ, 1998 લાગુ કરવામાં આવ્યો. આ કાયદો સૌ પ્રથમ વિવિધ વિકસીત દેશોના કાયદાઓનો આધાર લઈને તૈયાર કરવામાં આવ્યો અને ત્યારબાદ દેશના રાજયોની જરૂરીયાત અનુસાર તેમાં સુધારા કરવામાં આવ્યા. આ કાયદો બનાવતી વખતે તમામ પ્રકારની ઓનલાઈન પ્રવૃત્તિઓ અને તમામ ફરજો અને અધિકારોને ધ્યાનમાં રાખવામાં આવ્યા હતા અને પછી જ તેને માન્યતા આપવામાં આવી. ઈલેકટ્રોનિક કોમર્સ ઍક્ટ માન્ય ઈ-કોન્ટ્રાક્ટની મહત્ત્વની જરૂરિયાતો દર્શાવે છે. જે નીચે મુજબ છે.

- માન્ય ઈ-રેકોર્ડની હાજરી જરૂરી છે.
- તમામ ઈ-રેકોર્ડ સુરક્ષિત રાખવા જોઈએ.
- તમામ ઈ-રેકોર્ડ વિશ્વાસપાત્ર ડીજીટલ માધ્યમથી પ્રમાણિત થયેલ હોવા જોઈએ.
- વ્યવહારકર્તાઓ વચ્ચેનાં ઈલેકટ્રોનિક સંદેશા વ્યવહાર યોગ્ય સ્વરૂપમાં હાજર હોવા જોઈએ જેથી જરૂર મુજબ ઈ-કોન્ટ્રાક્ટને પ્રમાણીત કરવા તેનો ઉપયોગ કરી શકાય.

ઉપરોક્ત તમામ કાયદાઓને કારણે ભારતમાં ઈ-કોન્ટ્રાક્ટનું કાયદાકીય માળખું ખૂબ જ સુદ્રઢ થયું છે અને ઘણાબધા લોકો આજે જાણે-અજાણે વિવિધ રીતે ઈ-કોન્ટ્રાક્ટનો ભાગ બની રહ્યા છે.

1.6 ભારતમાં ઈ-કોન્ટ્રાક્ટની પરિસ્થિતિ

આપણે જોયું તે પ્રમાણે ભારતમાં બદલાતી જતી ટેક્નોલૉજીની સાથે દેશના વ્યાપાર તથા ઉદ્યોગને રાખવા સમયે કાયદમાં પણ ઉત્સાહક સુધારા વધારા થતા આવ્યા છે જેને ભારતમાં ઈ-કોન્ટ્રાક્ટનાં ઉપયોગને પ્રોત્સાહન આપ્યું છે. અત્યાર સુધીમાં ભારતમાં ઈ-કોન્ટ્રાક્ટ સરળતાથી અને સુરક્ષિતરૂપે થઈ શકે તે માટે નીચે મુજબના ઘણા બધા ભારતીય પ્લેટફોર્મ ઉપયોગમાં લેવામાં આવ્યા છે.

1.6.1. Zoho Sign: Zoho Sign એ ક્લાઉડ-આધારિત સોફ્ટવેરના સ્યુટનો એક ભાગ છે. તે ઈ-સિગ્નેચર, ડોક્યુમેન્ટ ઓટોમેશન અને કોન્ટ્રાક્ટ મેનેજમેન્ટ માટે સુવિધાઓ પ્રદાન કરે છે. તે નાના અને મધ્યમ કદના વ્યવસાયોમાં ઈ-કોન્ટ્રાક્ટ સુચારુરૂપે થઈ શકે તે માટે માટે રચાયેલ છે.

1.6.2. eMudhra : eMudhra એ ભારતીય ડિજિટલ વ્યવહારો માટે સુરક્ષા ઉકેલો (Security Solutions)નાં પ્રદાતા છે. તેઓ ઈ-સિગ્નેચર સેવાઓ, ડિજિટલ પ્રમાણપત્રો અને દસ્તાવેજની ચકાસણી કરવા માટેના ઉકેલો (Solutions) ઓફર કરે છે.

1.6.3. LegalDesk : LegalDesk એ એક ભારતીય પ્લેટફોર્મ છે જે વપરાશકર્તાઓને ઓનલાઈન કાનૂની દસ્તાવેજો બનાવવા, તેમાં પોતાની જરૂરિયાત પ્રમાણે સુધારા વધારા (કસ્ટમાઇઝ) કરવા માટે પ્લેટફોર્મ આપે છે. તે વિવિધ પ્રકારના કરારો તથા અન્ય કાનૂની દસ્તાવેજો માટે તૈયાર નમૂનાઓ (ટેમ્પ્લેટ) પણ પ્રદાન કરે છે.

આ ઉપરાંત DocuSign, Adobe Sign, SignEasy, IBM Emptoris, SAP Ariba, Icertis, vComply વગેરે જેવા વૈશ્વિક પ્લેટફોર્મ પણ ઈ-કોન્ટ્રાક્ટ માટે ભારતમાં વિવિધ લોકો તથા કંપનીઓ દ્વારા ઉપયોગમાં લેવામાં આવે છે.

પ્રસ્તુત સમયમાં ભારતમાં Tata Consultancy Services (TCS), Reliance Industries Limited, ICIC Bank, ITC Limited, HCL Technologies, Bajaj Finance Limited વગેરે જેવી કંપનીઓ નીચે મુજબના કાર્યો માટે ઈ-કોન્ટ્રાક્ટ મેનેજમેન્ટ સોલ્યુશન્સનો ઉપયોગ કરી રહી છે.

- વૈશ્વિક કોન્ટ્રાક્ટ પ્રક્રિયાઓનું સુવ્યવસ્થિત કરવા.
- કોન્ટ્રાક્ટ પ્રોસેસિંગના સમયમાં નોંધપાત્ર ઘટાડો કરવા અને કોન્ટ્રાક્ટ લાઈફસાઈકલ મેનેજમેન્ટ પર વધુ સારું નિયંત્રણ હાંસલ કરવા.
- પ્રાપ્તિ કરાર (procutement contracts)ને ડિજિટાઈઝ કરવા, સપ્લાયર કરારો (supplier agreements)નું સંચાલન કરવા અને અનુપાલન (compliance)ને સરળ બનાવવા.
- કોન્ટ્રાક્ટ મેનેજમેન્ટમાં વધુ પારદર્શિતા લાવવા.
- KYC પ્રક્રિયાઓને સુવ્યવસ્થિત કરવા.
- લોન ઓરિજિનેશન પ્રક્રિયાને ડિજિટાઈઝ કરવા.

1.7 ઈ-કોન્ટ્રાક્ટના સંદર્ભમાં આંતરરાષ્ટ્રીય પરિસ્થિતિ

આગળ જોયું તે મુજબ ટૅક્નોલૉજીનાં વ્યાપની સાથે આજે સમગ્ર વિશ્વમાં ઈ-કોન્ટ્રાક્ટનું ચલન ખૂબ જ વધી રહ્યું છે. દુનિયાના લગભગ દરેક દેશોમાં ઓછા-વત્તા પ્રમાણમાં લોકો વિવિધ પ્રકારે ઈ-કોન્ટ્રાક્ટનો ઉપયોગ કરી રહ્યા છે.

1.7.1. USA માં ઈ-કોન્ટ્રાક્ટની પરીસ્થિતિઃ ઈલેકટ્રોનિક એકસચેન્જને કારણે આજે એકબીજાથી દૂર રહેલ વ્યક્તિઓ પણ એકબીજા સાથે ખૂબ જ ઝડપ અને સહેલાઈથી સંપર્ક કરી શકે છે અને ઈ-કોન્ટ્રાક્ટમાં જોડાઈ શકે છે. યુનિફોર્મ ઈલેક્ટ્રોનિક ટ્રાન્ઝેકશન ઍક્ટ (UETA)ને USA માં ઈ–કરાર માટે અધિકૃત કાયદા તરીકે માનવામાં આવે છે. યુનિફોર્મ ઈલેક્ટ્રોનિક ટ્રાન્ઝેકશન ઍક્ટની કલમ 3 અને 4 મુજબ આ કાયદો ફક્ત વ્યવસાય અને સરકારી બાબતોને લગતા સોદાઓ પર અમલ કરે છે વળી એવા વેપારો કે જે ઈલેક્ટ્રોનિક પદ્ધતિઓ દ્વારા કરવામાં આવે છે તેને પણ આ કાયદો લાગુ પડે છે. ત્યારબાદ USA માં U.C. ઈલેક્ટ્રોનિક સિગ્નેચર ઈન ગ્લોબલ એન્ડ નેશનલ કોમર્સ ઍક્ટ (ઈ–સાઈન ઍક્ટ), 2001 પણ લાગુ કરવામાં આવ્યો. આ કાયદો ઈલેક્ટ્રોનિક માધ્યમ દ્વારા કરવામાં આવતા વ્યવહારોની અધિકૃતતા માટે છે. વધુમાં, યુનિફોર્મ કોમ્પ્યૂટર ઈન્ફોર્મેશન ટ્રાન્ઝેકશન ઍક્ટ (UCITA) એ પ્રસ્તાવિત યુએસ કાયદાનો નોંધપાત્ર રેકોર્ડ છે જે ખાસ કરીને ડિજિટલ પ્લેટફોર્મ પરના ઈન્કોન્ટ્રેકટ માટે સુસંગત છે. આ UCITA ને વિવિધ રાષ્ટ્રો દ્વારા સ્વીકારવામાં આવ્યું હતું અને તેમાંના કેટલાક રાષ્ટ્રોએ આ કાયદામાં વિવિધ સુધારાઓ પણ કર્યા છે.

1.7.2. યુરોપિયન યુનિયનમાં ઈ–કોન્ટ્રાક્ટની પરિસ્થિતિ : યુરોપિયન યુનિયન દ્વારા તેમના આંતરિક બજારમાં ઈલેક્ટ્રોનિક વાણિજય માટે કાનૂની માળખું પૂરું પાડવા માટે ઈકોમર્સ ડાયરેકિટવ 2000/31/EC અપનાવવામાં આવ્યો છે. આ ડાયરેકિટવનો હેતુ યુરોપિયન યુનિયનનાં બે સભ્ય રાષ્ટ્રો વચ્ચે ઓનલાઈન સેવાઓનો ઉપયોગ કરતી વખતે સભ્ય રાષ્ટ્રોના લોકો વચ્ચે રહેલા અવરોધોને દૂર કરવાનો અને તેમને કાનૂની નિશ્ચિતતા પૂરી પાડવાનો છે. આ નિર્દેશનો હેતુ એ પણ છે કે જે લોકો યુરોપિયન યુનિયનની અંદર ઓનલાઈન કરાર કરે છે તેઓ તેમના આ પ્રકારના કરારના કાનૂની પરિણામોથી વાકેફ થાય અને તેઓ ભયમુકત થઈને વિશ્વાસથી આવા કરાર કરી શકે. યુરોપિયન યુનિયન એ ઘણાબધા સભ્ય દેશોનું બનેલું છે જેમાં પ્રત્યેક દેશનાં પોતાના રાષ્ટ્રીય કાયદાઓ છે, તેથી યુરોપિયન યુનિયન જે નિર્દેશો અપનાવે છે તે સભ્ય રાજયોએ ચોક્કસ ક્ષેત્રોમાં એકરૂપતા સુનિશ્ચિત કરવા માટે તેમના સ્થાનિક કાયદામાં સમાવિષ્ટ કરવા આવશ્યક છે. જો સભ્ય રાજય આમ કરવામાં નિષ્ફળ જાય, તો યુરોપિયન યુનિયન તેની સામે તાત્કાલિક પગલાં લઈ શકે છે.

1.7.3. મલેશિયામાં ઈ-કોન્ટ્રાક્ટની પરિસ્થિતિ : યુનાઈટેડ નેશન્સ કમિશન ઓન ઈન્ટરનેશનલ ટ્રેડ લો દ્વારા ધ મૉડેલ લૉ ઑન ઈલેક્ટ્રોનિક કોમર્સ (1996) તૈયાર કરવામાં આવ્યો જેનો મુખ્ય હેતુ આંતરરાષ્ટ્રીય સ્તરે માન્ય એવા કાયદાઓ આપવા જેના દ્વારા ઈલેકટ્રોનિક કોમર્સને અનુલક્ષીને કાયદાકીય રીતે ઉદ્‌ભવતા પડકારોને નિવારી શકાય. આજ કાયદાઓને લક્ષમાં લઈ મલેશિયાની સંસદ દ્વારા ઈલેક્ટ્રોનિક કોમર્સ ઍક્ટ (અધિનિયમ 658) 2006 ઘડવામાં આવ્યો. આ અધિનિયમનો હેતુ વ્યાપારી વ્યવહારોમાં ઈલેક્ટ્રોનિક સંદેશાઓને કાનૂની માન્યતા આપવી અને કાનૂની આવશ્યકતાઓને પૂર્ણ કરવા માટે ઈલેક્ટ્રોનિક સંદેશાઓનો ઉપયોગ અને ઈલેક્ટ્રોનિક માધ્યમોના ઉપયોગ દ્વારા વ્યવસાયિક વ્યવહારોને સક્ષમ બનાવવાનો હતો. આ ઉપરાંત મલેશિયામાં ઓનલાઈન વ્યવહારોનું નિયમન કરવા માટે ઈલેક્ટ્રોનિક ગવર્નમેન્ટ એકિટવિટી ઍક્ટ, 2007 (GAA) અને ડિજિટલ સિગ્નેચર ઍક્ટ, 1997 (DSA) જેવા ઘણા કાયદા ઘડ્યા છે.

- **સારાંશ :**

ઈ-કોમર્સ અને ઈ-કોન્ટ્રેક્ટ પર આધુનિક ડિજિટલ યુગના અનિવાર્ય પાસાઓ બની ગયા છે. ઈ-કોમર્સ એટલે ઈન્ટરનેટના માધ્યમથી વેપાર કરવાની પ્રક્રિયા, જેમાં ઓનલાઈન ખરીદી, વેચાણ અને ચૂકવણીનો સમાવેશ થાય છે. જ્યારે ઈ-કોન્ટ્રેક્ટ એટલે ઈલોક્ટ્રોનિક માધ્યમથી થતો કોઈપણ કરાર, જેમ કે, ઈ-મેલ કે વેબસાઈટ દ્વારા. આ બંને તકનિકો વેપાર અને વાણિજ્યમાં ક્રાંતિ લાવી છે. ઈ-કોમર્સ ગ્રાહકોને ઘરબેઠા વિશ્વભરની વસ્તુઓ ખરીદવાની સુવિધા આપે છે, જ્યારે ઈ-કોન્ટ્રેક્ટ વ્યવસાયિક કામગીરીને ઝડપી અને કાર્યક્ષમ બનાવે છે. જોકે, આ તકનિકો સાથે સાયબર સુરક્ષાના જોખમો પણ સંકળાયેલા છે. હેકિંગ, ઓનલાઈન છેતરપિંડી અને ડેટા ચોરી જેવા સાયબર અપરાધો ઈ-કોમર્સ અને ઈ-કોન્ટ્રાક્ટ માટે મોટો ખતરે બની શકે છે. આ સમસ્યાઓને ઘટાડવા માટે મજબૂત સાયબર સુરક્ષા પગલાં અને કાયદાકીય માળખું જરૂરી છે. ઈ-કોમર્સ અને ઈ-કોન્ટ્રેક્ટના ફાયદાઓનો લાભ લેવા માટે, વ્યક્તિઓ અને વ્યવસાયોએ સાયબર સુરક્ષાના મહત્ત્વને સમજવું જોઈએ અને તેને ગંભરતાથી લેવું જોઈએ.

1.8 તમારી પ્રગતિ ચકાસો.

1. ઈ-કોન્ટ્રાક્ટની એટલે શું ?

2. ઈ-કોન્ટ્રાક્ટનાં કોઈપણ ત્રણ ફાયદા જણાવો.

3. ઈ-કોન્ટ્રાક્ટનાં પ્રકારો જણાવો.

4. ઈ-કોન્ટ્રાક્ટની પરિપૂર્ણતા માટેની આવશ્યકતાઓ જણાવો.

5. ભારતમાં ઈ-કોન્ટ્રાક્ટની માન્યતા અને ઈ-કોન્ટ્રાક્ટને લગતા પ્રશ્નોનાં નિરાકરણ માટે ઉપયોગી કાયદાઓ જણાવો.

____

____

____

1.9 ચાવીરૂપ શબ્દો

- **ઓનલાઈન દસ્તાવેજો :** એવા દસ્તાવેજો કે જે દુનિયામાં ગમે તે જગ્યાએથી ઈન્ટરનેટ સાથે જોડાયેલ યંત્રથી ગમે ત્યારે ઉપયોગમાં લઈ શકાય.
- **પક્ષકારો :** કોઈપણ વ્યવહારમાં (ખરીદવું, વેચવું, વગેરે) જોડાયેલ વ્યક્તિ
- **ઈ-કોમર્સ :** ડિજિટલ માધ્યમની મદદથી ઓનલાઈન કરવામાં આવતી ખરીદી કે વેચાણની પ્રક્રિયા.
- **ઈ-રેકોર્ડ :** એવી માહિતી કે જે સર્વરમાં સંગ્રહી રાખેલી હોય અને તેને માન્ય વ્યક્તિ ઈન્ટરનેટની મદદથી જરૂર પ્રમાણે ઉપયોગ કરી શકે.
- **KYC પ્રક્રિયાઓ :** કોઈ એક પક્ષકાર દ્વારા પોતાની વસ્તુ ખરીદનાર અથાવ તો સર્વિસનો ઉપયયો કરનાર બીજા પક્ષકારની ખરાઈ કરવાની પ્રક્રિયા (KYC : Know Your Customer)

1.10 સંદર્ભસૂચિ

1. Dr. R K Singh, Law Relating to Electronic Contracts, LexisNexis Publication
2. Dr. Sachin Rastogi, Insights into E-Contracts in India, LexisNexis Publication
3. Namrata Shukla, E-Contracts Tenders & Agreements, Lawmann's Publication
4. Dr. Deo John Nangela, E-Commerce & E-Contracting Law

એકમ-2 ભારતમાં મોબાઈલ કાયદા

: રૂપરેખા :

2.0 ઉદ્દેશ

2.1 મોબાઈલ અપરાધ

2.2 મોબાઈલ ફોનનો ઉપયોગ અને ડ્રાઈવિંગ

2.3 મોબાઈલ અને તેનો સ્માર્ટ વપરાશ

2.4 મોબાઈલ અપરાધ સામે નિવારણ અને રક્ષણ

2.5 મોબાઈલ ફોન અને ઈન્ટરનેટ

● સારાંશ

2.6 તમારી પ્રગતિ ચકાસો

2.7 ચાવીરૂપ શબ્દો

2.6 સંદર્ભસૂચિ

2.0 ઉદ્દેશ

વિદ્યાર્થીમિત્રો, આ પ્રકરણનો અભ્યાસ કર્યા બાદ તમે;

- મોબાઈલને લગતા ગુનાઓ વિશે જાણશો.
- વાહન ચલાવતી વખતે મોબાઈલ ફોનના ઉપયોગને લગતા નિયમો સમજશો.
- મોબાઈલ ફોનના સ્માર્ટ ઉપયોગ કરી શકશો.
- મોબાઈલને લગતા ગુનાઓનું નિવારણ તથા તેની સામે રક્ષણ કઈ રીતે થઈ શકે તે જાણીશું
- મોબાઈલ ફોન દ્વારા ઇન્ટરનેટના ઉપયોગ વિશે માહિતી મેળવશો.

2.1 મોબાઈલ અપરાધ

ભારતમાં ટેલિકોમ્યુનિકેશનની શરૂઆત વર્ષો પહેલાં થઈ હતી. 1882 પછી ટેલિકોમ્યુનિકેશનમાં ખૂબજ ઝડપી વૃદ્ધિ જોવા મળી અને તેથી ભારતમાં ઈન્ટરનેટ અને મોબાઈલ ટૅક્નોલૉજીનું આગમન થયું. ઓગસ્ટના 15, 1995 ના રોજ પ્રથમ મોબાઈલ ટેલિફોન સેવા બિનવ્યવસાયિક ધોરણ પર શરૂ થઈ. એ જ દિવસે ભારતમાં ઈન્ટરનેટનું પણ આગમન થયું. આ ક્ષેત્રમાં મુક્તિ અને ખાનગીકરણ પછી ભારતે પાછું વળીને જોયું નથી. ટેલિકોમ્યુનિકેશને રોજિંદા જીવન પર પ્રભાવ પડ્યો અને ટૂંક સમયમાં ભારતનું ટેલિકોમ્યુનિકેશન નેટવર્ક વિશ્વમાં બીજા નંબરનું સૌથી મોટું નેટવર્ક બની ગયું. હવેના સમયમાં જો કોઈ વ્યક્તિ મોબાઇલ–યુઝર ન હોય તો તે આશ્ચર્ય કહેવાય.

સમયાંતરે અહેવાલોએ સૂચવ્યું છે કે ટેલિકોમ્યુનિકેશન ટૅક્નોલૉજીની પ્રગતિને કારણે દેશમાં સાયબર અપરાધમાં વધારો થયો છે. તકનીકી પ્રગતિએ અમુક અસામાજિક તત્ત્વોને તકો પૂરી પાડી છે જેનો તેઓ પોતાના સ્વાર્થ માટે ઉપયોગ કરી રહ્યા છે. વિવિધ ઓપરેટીંગ

સિસ્ટમ જેમકે નોકીઆની સિમ્બિયન, એપલની job અને ગૂગલની એન્ડ્રોઇડ ઓપરેટિંગ સિસ્ટમ કે તેના પર ચાલતી એપ્લીકેશન (Application) હેકર્સ દ્વારા હેક થયાના કિસ્સાઓ છે. આથી મોબાઈલ યુઝરે સલામત તથા જાગૃત રહેવું જોઈએ. સાયબર અપરાધ વિશેની પાયાની સમજ દરેક પ્રકારના મોબાઇલ ઉપયોગકર્તા માટે આજના સમયમાં ખૂબ જ જરૂરી છે. અમુક યુઝર્સ કે જેઓ માને છે કે તેઓ મોબાઈલનો ખૂબ જ સીમિત ઉપયોગ કરે છે અને તેથી તેઓને સાઈબર અપરાધથી કોઈ ખતરો નથી એવી માન્યતા ખોટી છે. સાઈબર અપરાધ વિવિધ પ્રકારે આચરવામાં આવે છે અને મોબાઈલના ઉપયોગમા થયેલી નાની ભૂલ પણ મોટુ નુકસાન પહોંચાડી શકે છે. ફક્ત ઇન્ટરનેટ નહીં પરંતુ બ્લુ ટૂથ અથવા તો ઇન્ફ્રા રેડ સક્ષમ સેલ ફોનનો ઉપયોગ કરતી દરેક વ્યક્તિ પણ સાયબર ગુનેગારોના જાળમાં ફસાઈ શકે છે. આથી જ દરેક પ્રકારના મોબાઇલ ઉપયોગ કર્તાએ સાઈબર અપરાધ વિશે અને તેનાથી બચવાના ઉપાયો વિશે માહિતગાર હોય તો જ સલામત રહી શકાય છે.

સમયાંતરે મળતા અહેવાલો અત્યંત સંગઠિત અને વ્યાવસાયિક સાયબર ક્રિમિનલ પ્રવૃત્તિ તરફ ચિંતાજનક પરિવર્તન સૂચવે છે. તેનાથી પણ વધુ ચિંતાજનક બાબત એ છે કે આપણા દેશમાં આ પ્રકારની પ્રવૃત્તિમાં મહદ અંશે વધારો જોવા મળેલ છે. લોકોની વધતી જતી સંખ્યા તેમના અન્ય ઉપકરણો કરતાં તેમના સ્માર્ટફોન દ્વારા વારંવાર ઇન્ટરનેટનો ઉપયોગ કરવામાં આવે છે. જો કે, જ્યારે મોટાભાગના લોકો પાસે તેમના ડેસ્કટોપ અને લેપટોપ પર પર્યાપ્ત એન્ટિવાયરસ અને અન્ય સુરક્ષા સિસ્ટમો ઇન્સ્ટોલ કરેલી હોય છે, ત્યારે તેમના સ્માર્ટફોન માટે એવું કહી શકાય તેમ નથી. પરિણામે, અત્યંત સંવેદનશીલ માહિતી હવે સ્માર્ટફોનમાંથી સાયબર અપરાધીઓ માટે વધુ સરળતાથી મળી રહે એમ છે. આ પરિબળોએ સ્માર્ટફોનને સાયબર અપરાધીઓ માટે અત્યંત આકર્ષક લક્ષ્ય બનાવ્યું છે.

મોબાઈલ ફોન સાથે સંકળાયેલ સામાન્ય સાયબર ક્રાઇમ્સ નીચે મુજબ છે.

1. બ્લુજકિંગ, બ્લુસ્નાર્ફિંગ અને બ્લુબગિંગ : નામ સૂચવે છે તેમ આ હુમલો બ્લૂટૂથ દ્વારા થાય છે. બ્લૂટૂથ ટૅક્નોલૉજી હવે લગભગ દરેક મોબાઇલ સેલ ફોન સાથે એમ્બેડેડ હોય છે. યુઝર દ્વારા ફોટા, ઓડિયો અથવા વિડિયો ફાઈલો શેર કરવા માટે બ્લૂટૂથનો ઉપયોગ બ્લુબગિંગ હેકરને કબજો મેળવવાની મંજૂરી આપે છે અને તેના થકી હેકર મોબાઇલ ફોન પર સંપૂર્ણ નિયંત્રણ મેળવી લે છે. બ્લુબગિંગથી હેકર તમારા મોબાઇલ ફોનમાં માહિતી વાંચી શકે છે, તે કેલેન્ડર, એડ્રેસ બુક વગેરે ઍકસેસ કરી શકે છે, તે કોલ કરી શકે છે અને મોકલી પણ શકે છે, હેકર તમારી વાતચીત પણ સાંભળી શકે છે. બ્લુજેકિંગનો ઉપયોગ અન્ય બ્લૂટૂથ ઉપકરણ પર અનધિકૃત સંદેશા મોકલવા માટે થાય છે. બીજી તરફ બ્લુસ્નાર્ફિંગ એ બ્લૂટૂથ કનેક્શન સાથે જોડાયેલા ઉપકરણમાંથી ગેરકાયદેસર રીતે માહિતીની ચોરી કરવાનું કાર્ય છે. બ્લુબગિંગ બ્લુજેકિંગ અથવા બ્લુસ્નાર્ફિંગથી આગળ બધી, ઉપકરણ પર સંપૂર્ણ નિયંત્રણ મેળવી શકે છે.

2. ફિશિંગ : આ નાણાકીય ગુનો કરવા માટેની એક પદ્ધતિ છે. ફિશિંગ આજના સમયમાં ખૂબ જ પ્રચલિત છે. મોબાઈલ ફોનનો ઉપયોગ હવે ઓનલાઈન શોપિંગ અને બેંકિંગ વ્યવહારો મેનેજ કરવા માટે થાય છે. આનાથી મોબાઈલ સેલ ફોન ફિશિંગનો સરળ શિકાર બની ગયો છે. અહીં હેકરનો હેતુ સરળતાથી પૈસા મેળવવાનો હોય છે. આ હુમલા ફિશીંગ હુમલા જેવા જ છે. તેમાં ઓળખની ચોરીનો સમાવેશ થાય છે જેમ કે ક્રેડિટ કાર્ડ નંબર અને અન્ય ગુપ્ત માહિતી. આ કિસ્સામાં હેકર મોબાઈલ યુઝર પાસેથી ફોન કોલ દ્વારા એમની ગુપ્ત માહિતી મેળવવાનો પ્રયત્ન કરે છે. આથી દરેક વ્યક્તિએ કોઈપણ પ્રકારના ફોન કોલ કે જે આકર્ષક ઓફર અથવા સ્કીમ દ્વારા ગુપ્ત માહિતી મેળવવાનો પ્રયત્ન કરે

તેનાથી સાવધ રહેવું જોઈએ.

3. માલવેર : સ્માર્ટફોન સંબંધિત સાયબર અપરાધ કરવા માટેનું પ્રથમ પગલું એ તેના પર માલવેર ઇન્સ્ટોલ કરવું છે. મોબાઈલ સેલ ફોન માટે આ સૌથી મોટો ખતરો છે. તે દૂષિત પ્રવૃત્તિઓ કરવા માટે રચાયેલ પ્રોગ્રામ (સોફ્ટવેર) છે. માલવેર એસએમએસ, ફાઇલ ટ્રાન્સફર, ઈન્ટરનેટ પરથી પ્રોગ્રામ ડાઉનલોડિંગ વગેરે દ્વારા મોબાઈલ ફોનમાં પ્રવેશે છે. માલવેર ફોનમાં ઉપયોગ કર્તાની જાણ બહાર પ્રવેશે છે અને ફોનને નુકસાન પહોંચાડવાનું કાર્ય કરે છે, માલવેર મોબાઇલમાં સ્ટોર કરેલ માહિતી પણ યુઝરની જાણ બહાર અન્ય જગ્યા પર મોકલવાનું કાર્ય કરે છે.

4. સ્મિશિંગ : આજના સમયમાં એસ.એમ.એસ (SMS) મોબાઇલ ફોન પર સંદેશાઓ શેર કરવા માટે એક પ્રચલિત માધ્યમ છે. આ સેવા મોબાઇલ ફોન પર સૌથી વધુ ઉપયોગમાં લેવાતી સેવામાંની એક છે. તેથી ગુનેગારો તેમના લોભને સંતોષવા માટેના સાધન તરીકે તેને લક્ષ્ય બનાવી રહ્યા છે. આ એક સિક્યોરિટી એટેક છે જેમાં યુઝરને એસએમએસ મોકલવામાં આવે છે. આ એસએમએસ નફાકારક સેવા છે એવું બતાવી યુઝરને તેમની અંગત માહિતી આપવા માટે પ્રેરિત કરે છે, જેનો પાછળથી દુરુપયોગ થાય છે. આ તરકીબ મોબાઇલમાં માલવેર દાખલ કરવા માટે પણ ઉપયોગમાં લેવાય છે. આ ફિશિંગ અને વિશિંગ હુમલાઓ એકસરખા છે જેમાં વ્યક્તિગત ગોપનીય માહિતી મેળવવામાં આવે છે અને બાદમાં તેનો દુરુપયોગ થાય છે. આ હુમલાઓમાં ગુનેગાર ઇન્ટરનેટ બેંકિંગ પાસવર્ડ્સ, ક્રેડિટ કાર્ડની વિગતો, ઈમેલ આઈડી અને પાસવર્ડ વગેરે મેળવે છે.

મોબાઇલ ઉપકરણો પર ફિશિંગ એ ફિશિંગનું એક નવું સ્વરૂપ છે જ્યાં માલવેરને કારણે નકલી લોગિન પેજ કાયદેસર લોગીન પેજની ઉપર પોપ અપ થાય છે. આનાથી વપરાશકર્તાઓ તેમની લૉગિન વિગતો દાખલ કરવામાં છેતરાય છે, અને લોગિનની વિગતો હેકરને મળી જાય છે.

5. ઉપકરણની નબળાઈઓનું શોષણ : માલવેરના સરળ ઇન્સ્ટોલેશનને સક્ષમ કરવા માટે સાયબર અપરાધીઓ દ્વારા મોબાઇલ ઉપકરણની નબળાઈઓનો ઉપયોગ કરવામાં આવે છે. ઉદાહરણ તરીકે, જુલાઇ 2015 માં એક નબળાઈ મળી આવી હતી જ્યાં ફક્ત વપરાશકર્તાઓને મોકલવામાં આવેલ દૂષિત વીડિયો સંદેશને જોવાથી તેમના ઉપકરણો પર શોષણ થઈ જતું હતું. આ રોકવા ઓપરેટિંગ સીસ્ટમ બનાવતી કંપનીએ તરત જ પેચ બહાર પાડ્યો હતો, પણ કેરિયર્સ અને ઉપકરણ ઉત્પાદકોએ તેમના વપરાશકર્તાઓને પેચ પ્રદાન કરવામાં થોડા અઠવાડિયાથી થોડા મહિનાનો સમય લીધો. આનાથી એક નવી સમસ્યા સામે આવી, જ્યાં ઉપકરણ ઉત્પાદકો દ્વારા કરવામાં આવેલા વિલંબને કારણે સમસ્યાની શોધ હોવા છતાં ઉપકરણો સતત નબળા રહેવાનું કારણ બને છે.

6. મેડવેર : એપ્સમાં જાહેરાત એ એપ્સ માટે ધિરાણ મેળવવાની સામાન્ય રીતે ઉપયોગમાં લેવાતી પદ્ધતિ છે. આમાં સામાન્ય રીતે એપ્લિકેશનમાં તૃતીય-પક્ષ એડવેરનું (Third party adware) એકીકરણ શામેલ હોય છે. દૂષિત એડવેર, ઉર્ફે મેડવેર, નું ચલણ આજના સમયમાં ખૂબ પ્રમાણમાં વધ્યું છે. ઉદાહરણ તરીકે, કુલ 256 જેટલી iOS એપમાં મેડવેર ‘Youmi’ શોધાયું હતું, જે યુઝર્સની અંગત માહિતીને પરવાનગી વિના અન્ય સ્થળોએ મોકલતું હતું. મેડવેર ઘણીવાર ચેપગ્રસ્ત ઉપકરણ પર અન્ય માલવેરના ઇન્સ્ટોલેશન તરફ દોરી જાય છે. મેડવેરનું ઇન્સ્ટોલેશન અગાઉના માલવેર ઇન્સ્ટોલેશનની ચર્ચા કરતા થોડું અલગ છે. કારણ કે પ્રારંભિક એપ જેમાં મેડવેર હાજર હતો તે માલિકની પરવાનગીથી ઇન્સ્ટોલ કરવામાં આવી હતી. ઘણી વાર, એપ્લિકેશનના નિયમો અને શરતો જાહેરાતો ઓફર કરવા માટે

વપરાશકર્તાની સંમતિ લે છે. જો કે, દૂરના સ્થાન પર ખનગી વિગતો જેમકે સંપર્ક વિગતો અને ભૌગોલિક સ્થાનીય માહિતી મોકલવી, એપ્લિકેશન માલિક દ્વારા આપવામાં આવેલી અધિકૃતતા બહારનું કાર્ય છે.

7. રેન્સમવેર : ખંડણીની ચૂકવણી ન થાય ત્યાં સુધી ફોનને એપ દ્વારા લોક રાખવાથી માંડીને ફોન પરના ડેટાને પણ એન્ક્રિપ્ટ કરવા માટે રેન્સમવેર નો ઉપયોગ થાય છે.

8. નકલી ટેક સપોર્ટ : આમાં સ્માર્ટફોનના ઉપયોગ પર એક પોપ-અપનો આવે છે જે વપરાશકર્તાઓને ગંભીર ભૂલ અથવા સમસ્યા વિશે ચેતવણી આપે છે, જે પછી તેમને ‘ટેક સપોર્ટ પ્રતિનિધિ’ નો સંપર્ક કરવા આમંત્રણ આપે છે. અધિકૃત દેખાતા સંદેશઓ લોકોને સફળતાપૂર્વક અમુક નંબર પર કૉલ કરવા અને નકામી સેવાઓ ખરીદવા માટે પ્રેરે છે. આના દ્વારા વ્યક્તિ ખોટી માહિતી આપી દે છે અથવા ખોટી જગ્યાએ પૈસા અપી દેતા હોય છે.

2.2 મોબાઈલ ફોનનો ઉપયોગ અને ડ્રાઈવિંગ

માર્ગ પરિવહન અને ધોરીમાર્ગ મંત્રાલય પ્રમણે વાહન ચલાવતી વખતે મોબાઈલ ફોનનો ઉપયોગ ફક્ત રૂટ નેવિગેશન માટે થઈ શકે છે, અને એ પણ ‘ડ્રાઈવરની એકાગ્રતામાં ખલેલ પહોંચાડ્યા વિના’ થાય એ જરૂરી છે.

ડ્રાઈવરો વાહન ચલાવતી વખતે ફક્ત નેવિગેશન માટે હેન્ડ હેલ્ડ ડિવાઈસ (મોબાઈલ ફોન) નો ઉપયોગ કરી શકે છે. ડ્રાઈવિંગ કરતી વખતે હેન્ડ હેલ્ડ ડિવાઈસ અથવા મોબાઈલ ફોનના ઉપયોગને સ્પષ્ટ કરતાં, મંત્રાલયના નોટિફિકેશનમાં કહેવામાં આવ્યું છે કે આનો ઉપયોગ ફક્ત વાહનના ડેશબોર્ડ પર ઉપકરણને ફિકસ કરીને રૂટ નેવિગેશન માટે જ હોય તો તેને મંજૂરી આપવામાં આવશે. ડ્રાઈવિંગ કરતી વખતે ડ્રાઈવરની એકાગ્રતામાં ખલેલ ન પહોંચે તેવી રીતે વૈશ્વિક અભ્યાસો સૂચવે છે કે ડ્રાઈવિંગ કરતી વખતે મોબાઈલ ફોનનો ઉપયોગ કરતા ડ્રાઈવરો ખાસ કરીને જોખમી ગણાતા. ડ્રાઈવિંગ દરમિયાન ટેકિસટંગ સાથે અકસ્માતમાં સામેલ થવાની સંભાવના લગભગ ચાર ગણી વધારે છે. ડ્રાઈવિંગ કરતી વખતે મોબાઈલ ફોનનો ઉપયોગ સંશોધિત મોટર વાહન અધિનિયમમાં જોખમી ડ્રાઈવિંગ શ્રેણી હેઠળ લાવવામાં આવ્યો છે અને તેને 5,000 રૂપિયા સુધીનો દંડ અથવા એક વર્ષની જેલ અથવા બંનેની જોગવાઈ છે.

2.3 મોબાઈલ અને તેનો સ્માર્ટ વપરાશ

માનવ જીવન પર સેલ ફોનની અસર વિશે એમ કહેવાય છે કે કોમ્યુનિકેશન ટૅક્નોલૉજીએ માનવ જીવનનું કોઈ પાસું છોડ્યું નથી. મોબાઈલ સેલ ફોન ટૅક્નોલૉજી સતત પ્રગતિ લાવી રહી છે.

મોબાઈલ ફોન હવે નવા પ્રકારના લેપટોપ કે ડેસ્કટોપ બની ગયા છે જેની ક્ષમતા લેપટોપ કે ડેસ્કટોપ જેટલી જ છે. ઈન્ટરનેટમાં ઝડપી વૃદ્ધિ તથા ઈન્ટરનેટ સક્ષમ મોબાઈલ ફોનના કારણે ઘણી બધી સેવાઓ ખૂબ જ સરળ બની ગઈ છે. આ સેવાઓ જેવીકે બેંકિંગ વ્યવહાર, સત્તાવાર અને સંસ્થાકીય વ્યવહારો, ઝડપી ઈ-મેઈલ અથવા સામાજિક નેટવકર્સ દ્વારા સંચાર, અને ઘણું બધું કામ આપણે આંગળીના ટેરવે કરી શકીએ છીએ. વર્ચ્યુઅલ રીતે આપણે આપણા મોબાઈલ પર કમ્પ્યૂટરનું કાર્ય કરી શકીએ છીએ, એનો અર્થ એ પણ છે કે આપણા કમ્પ્યૂટરની જેમ જ આપણો મોબાઈલ ફોન પણ ખૂબ સંવેદનશીલ છે, અને એના પર વિવિધ પ્રકારે સાયબર એટેક થઈ શકે છે.

સ્માર્ટફોન આપણા જીવનનો એક મહત્ત્વપૂર્ણ ભાગ બની ગયો છે અને તેના વિના આપણે ફક્ત અડધા વ્યક્તિ જેવા હોવાનું અનુભવીએ છીએ. સ્માર્ટફોન્સ આપણે જે રીતે વાતચીત કરીએ છીએ, માહિતી ઍકઠી કરીએ છીએ, વર્તીએ છીએ, અનુભવીએ છીએ અને અન્ય ટૅક્નોલૉજીનો ઉપયોગ કરીએ છીએ તે રીતે બદલાય છે

આપણામાંના મોટાભાગના લોકો દરરોજ તેમના સ્માર્ટફોનનો ઉપયોગ, ઈન્ટરનેટ અને સોશિયલ મીડિયા પ્લેટફોર્મ્સ સર્ફ કરવા, ઇ-મેઇલ્સ તપાસવા, કેલેન્ડર મેનેજ કરવા, સંગીત સાંભળવા, ગેમ્સ રમવા, વિડીયો જોવા, ફોટા લેવા, સમાચાર વાંચવા, ટેક્સ્ટ સંદેશા લખવા માટે અને તેનો ઉપયોગ તેમના મૂળ હેતુ માટે, ફોન કૉલ કરવા માટે કરીએ છીએ. હવે આ બધી પ્રવૃત્તિઓ એક જ ઉપકરણનો ઉપયોગથી કરી શકાય છે. જો તમે 25 વર્ષ પહેલાંનો વિચાર કરો તો તેમાંના કેટલાક શક્ય પણ ન હતા. પરિણામે, સ્માર્ટફોને આપણી જીવનશૈલીમાં ધરખમ ફેરફાર કર્યો છે.

આપણે જે રીતે માહિતીનો ઉપયોગ કરીએ છીએ તે એકબીજા સાથે વાત કરીને અખબાર વાંચવાથી લઈને ટેલિવિઝન જોવા, કમ્પ્યુટર અને હવે સ્માર્ટફોનનો ઉપયોગ કરીને વેબ પર માહિતી એકત્ર કરવા સુધી બદલાઈ ગઈ છે. આજે આપણે ગમે ત્યાં હોઈએ, 24/7 કોઈપણ પ્રકારની માહિતી મેળવી શકીએ છીએ. તે બંને, અનુકૂળ અને જબરજસ્ત છે. સંચાર માટે પણ એવું જ છે. સ્માર્ટફોન આપણને સંચારની ઘણી રીતો પ્રદાન કરે છેઃ કૉલ્સ, ટેક્સ્ટ મેસેજિંગ, ઈન્સ્ટન્ટ મેસેજિંગ, ઇ-મેઇલ, સોશિયલ મીડિયા, બ્લોગ્સ વગેરે.

સ્માર્ટફોન દ્વારા આપણે ગમે ત્યારે કોઈપણ માહિતી મેળવી શકીએ છીએ તેની આપણા જીવનશૈલી પર ઘણી અસર પડે છે. કોલંબિયા યુનિવર્સિટીના એક અભ્યાસમાં જાણવા મળ્યું છે કે આપણે એવી માહિતી ભૂલી જઈએ છીએ જે આપણે જાણીએ છીએ કે આપણે સરળતાથી ફરીથી મેળવી શકીએ છીએ. ઉપરાંત, જ્યારે આપણને પ્રશ્નો પૂછવામાં આવે છે, ત્યારે આપણે વાસ્તવિક પ્રશ્ન વિશે વિચારવા અને તેનો જવાબ જાતે આપવાને બદલે ઈન્ટરનેટ પર જવાબ કેવી રીતે શોધી શકીએ તે વિશે વિચારીએ છીએ. મૂળભૂત રીતે, આપણે વધુ સુસ્ત થઈ રહ્યા છીએ, કારણ કે આપણે જાણીએ છીએ કે મોબાઈલ દ્વારા કોઈપણ સમયે તમામ પ્રકારની માહિતીને ઍકસેસ કરી શકીએ છીએ.

2.4 મોબાઈલ અપરાધ સામે નિવારણ અને રક્ષણ

સ્માર્ટફોન ગુનાઓ માટે ભારતીય સાયબર કાયદાની લાગુ પડતી જોગવાઇઓ નીચે મુજબ છે.

ઈન્ફોર્મેશન ટૅક્નોલૉજી ઍક્ટ, 2000 એ 'કમ્પ્યુટર' સંબંધિત સાયબર ક્રાઇમ્સની શ્રેણીની યાદી આપે છે. આ અધિનિયમની કલમ 2(1)(i) હેઠળ 'કમ્પ્યૂટર' શબ્દની વ્યાખ્યા તેના અવકાશમાં ખૂબ જ વ્યાપક છે. જ્યારે અગાઉના મોબાઇલ ઉપકરણો આ અવકાશમાં આવતા નથી, ત્યારે સ્માર્ટફોનની વ્યાપક ક્ષમતાઓ તેને આ વ્યાખ્યા હેઠળ ચોક્કસ રીતે આવે છે. પરિણામે, કોઈપણ કાયદો જે કમ્પ્યૂટર સામેના ગુનાને રક્ષણ આપે છે, તે સ્માર્ટફોન સામેના ગુનાને પણ રક્ષણ આપશે.

ભારતીય આઈટી ઍક્ટની (IT Act) કલમ 43(a) માલિકની અધિકૃતતા વિના સ્માર્ટફોન એકસેસ કરનાર કોઈપણ વ્યક્તિને સજા કરશે, અને કલમ 43(c) વાયરસ ઈન્સ્ટોલ કરવા પર સજા કરશે. આઈટી ઍક્ટ સ્માર્ટફોનમાં વાયરસના એકસેસ અથવા ઈન્સ્ટોલેશનના મોડને સ્પષ્ટ કરતું નથી. પરિણામે, માલવેર ઈન્સ્ટોલેશનનું દરેક નવું સ્વરૂપ કે જે શોધાયું છે, જેમ કે અહીં ચર્ચા કરવામાં આવી છે, તે IT ઍક્ટ દ્વારા આવરી લેવાનું ચાલુ રહેશે.

આ કલમ હેઠળ દોષિત ઠરેલો સાયબર અપરાધી પીડિતને વળતર ચૂકવવા માટે જવાબદાર રહેશે. વ્યક્તિને ખોટી રીતે નુકસાન પહોંચાડવાના ઈરાદાથી આવું કરનાર વ્યક્તિ, ઉદાહરણ તરીકે, પીડિતાની બેંકિંગ લોગિન વિગતોની ચોરી કરવા માટે, કલમ 66 હેઠળ 3 વર્ષ સુધીની કેદ અને રૂ. 5 લાખ સુધીનો દંડ પણ થઈ શકે છે. અમુક એપ્લિકેશન્સ, દૂરસ્થ સ્થાન પર સંપર્ક વિગતો અને ભૌગોલિક સ્થાનીય માહિતી જેવી ખાનગી માહિતી મોકલવા જેવી ક્રિયાઓ કરીને, માલિક દ્વારા આપવામાં આવેલી અધિકૃતતાને વટાવી ગઈ કહેવાય, આથી એને પણ IT ઍક્ટની કલમ 43(a) અને (c) હેઠળ આવરી લેવામાં આવશે.

ફિશિંગને પરંપરાગત રીતે Act ઍક્ટની કલમ 66A(c) હેઠળ સજા કરવામાં આવતી હતી. સુપ્રીમ કોર્ટ દ્વારા કલમ 66a નાબૂદ થતાં, આ ખાસ ઉપાય ખોવાઈ ગયો છે. જો કે, અન્ય કલમો છે, જેમ કે કલમ 66C, જે ઓળખની ચોરીને સજા આપે છે, અને કલમ 66D, જે વ્યક્તિત્વ દ્વારા છેતરપિંડી કરવા માટે સજા આપે છે. આ માટે 3 વર્ષ સુધીની જેલ અને 1 લાખ રૂપિયા સુધીના દંડની સજા છે. અગાઉ ઉલ્લેખ કર્યો છે તેમ, IT ઍક્ટનો વ્યાપ એટલો બહોળો છે કે તે શોધાયેલ આ પ્રકાર સહિત કોઈપણ નવા પ્રકારની ફિશીંગને સમાવી શકે.

રેન્સમવેર Act ઍક્ટની કલમ 43(F) સાથે વાંચેલી કલમ 66 હેઠળ આવરી લેવામાં આવ્યું છે. આ વિભાગ સાયબર ક્રિમિનલ દ્વારા સ્માર્ટફોનના ઉપયોગકર્તાને એકસેસ નકારવા પર સજા આપે છે, તે ખંડણી મેળવવાના ઈરાદાથી કરવામાં આવ્યું હોવાથી, તેને 3 વર્ષ સુધીની જેલ અને 5 લાખ રૂપિયા સુધીના દંડની સજા થઈ શકે છે. ઉપર ચર્ચા કર્યા મુજબ IT ઍક્ટની કલમ 66D હેઠળ નકલી ટેક સપોર્ટ સ્કેમ્સ પણ સુરક્ષિત છે.

એ એકદમ સ્પષ્ટ છે કે IT ઍક્ટ તદ્દન અસરકારક રીતે વિવિધ સાયબર અપરાધ સામે રક્ષણ આપે છે. બીજી બાજુ, ગુનેગારોને દોષિત ઠેરવવું એ ખૂબ મુશ્કેલ કાર્ય છે. લોકોએ હવે પુરાવાના સંગ્રહ અને સાયબર અપરાધના તાત્કાલિક રિપોર્ટીંગના સ્વરૂપમાં પણ તેમની ભૂમિકા ભજવવાની જરૂર છે. નિયમિત ડેટા બેકઅપ લેવા અને સમયસર અપડેટ કરવા જેવા કેટલાક સરળ પગલાં યુઝરને સુરક્ષિત રાખવા માટે ખૂબ ઉપયોગી રહેશે.

સેલ ફોનને સુરક્ષિત કરવા માટેની ટિપ્સ

- જ્યારે જરૂરી હોય ત્યારે જ બ્લૂટૂથ ચાલુ કરો અથવા ઇન્ટરનેટ ચાલુ કરો.
- જ્યારે જરૂર ન હોય ત્યારે વાયરલેસ જોડાણો બંધ કરો,
- સેલ ફોન સોફ્ટવેરને નિયમિતપણે અપડેટ કરો.
- નવીનતમ એન્ટિ-વાયરસ સોફ્ટવેર ઇન્સ્ટોલ કરો અને તેને અપડેટ રાખો.
- તમારા સેલ ફોનને લોક કરવા માટે મજબૂત પાસવર્ડનો ઉપયોગ કરો.
- અજાણી વ્યક્તિ સાથે ક્યારેય અંગત માહિતી શેર કરશો નહીં.
- સેલ ફોનમાં વ્યક્તિગત બેંકિંગ વિગતો ક્યારેય સંગ્રહિત કરશો નહીં.
- સામાજિક નેટવર્કિંગ વેબસાઈટ પર અજાણ્યાઓ સાથે વાતચીત કરતી વખતે શંકાસ્પદ બનો.
- તમારા ફોન પર જિયો-ટેગિંગ સુવિધાને અક્ષમ કરવાનું વિચારો.
- જો તમે સાર્વજનિક WiFi સાથે કનેક્ટેડ છો, તો જ્યાં તમારે પાસવર્ડ, ક્રેડિટ કાર્ડ માહિતી વગેરે દાખલ કરવાની જરૂર છે એવી સાઈટ્સ ઍક્સેસ કરશો નહીં.

- બેંકિંગ અને ઓનલાઈન ખરીદી કરતી વખતે, ખાતરી કરો કે સાઇટ્સ https અથવા shttp છે.

2.5 મોબાઈલ ફોન અને ઈન્ટરનેટ

આજકાલ, સેલ્યુલર ફોન યુઝર્સને ચાલતા-ફરતા ઇન્ટરનેટ ઍક્સેસ કરવાની મંજૂરી આપે છે. મોબાઇલ ફોન સેલ્યુલર ટેલિફોન કે ડેટા સર્વિસ પ્રોવાઇડર અથવા વિશિષ્ટ ટૅક્નોલૉજી દ્વારા ઇન્ટરનેટને સપોર્ટ કરે છે, જેવા કે WAP (વાયરલેસ એક્સેસ પ્રોટોકોલ) અને વાઇ—ફાઇ (વાયરલેસ લોકલ એરિયા નેટવર્ક). મોબાઈલ ઈન્ટરનેટ સાથે, તમે અદ્યતન રહી શકો છો. તમને હંમેશા નવીનતમ માહિતી અને ડેટાની ઍક્સેસ મળશે. સમગ્ર વિશ્વમાં આશરે 500 મિલિયનથી વધુ લોકો મોબાઈલ ઈન્ટરનેટનો ઉપયોગ કરી રહ્યા છે. મોબાઇલ ઈન્ટરનેટના કેટલાક ફાયદા અને ગેરફાયદા છે,

- **મોબાઈલ ઈન્ટરનેટના ફાયદાઓ**

અપડેટેડ રહો મોબાઇલ ઇન્ટરનેટ સાથે, યુઝર્સ હંમેશાં અપડેટેડ રહી શકે છે. માહિતી નવી સાઇટ્સની મુલાકાત લેવાથી, બ્રેકિંગ ન્યૂઝ વાંચવા અને વ્યવસાયની માહિતી સુધીની હોઈ શકે છે. યુઝર્સ મુસાફરીના અપડેટ્સ, હવામાનની આગાહીઓ અને શેરની કિંમતો વિશેની વિસ્તૃત માહિતી મેળવી શકે છે. અપડેટ કરેલી માહિતી સાથે, સાચો નિર્ણય લઈ શકે છે.

(1) તમારી જાતને શોધો - મોબાઇલ ઇન્ટરનેટ વિવિધ ક્ષેત્રોમાં નવી માહિતી શોધવામાં મદદ કરે છે. દાખલા તરીકે, નજીકના પર્યટન સ્થળો, રેસ્ટોરન્ટ અને કલબ્સ વગેરે શોધી આપી શકે છે. યુઝર્સ ભલામણો મેળવી શકે છે અને નકશા પર સ્થાનો શોધી શકે છે. હવે લગભગ દરેક ફોનમાં GPS (ગ્લોબલ પોઝિશનિંગ સિસ્ટમ) હોય છે જે ફોનના વપરાશકર્તાઓને શોધવા માટે સેટેલાઇટનો ઉપયોગ કરે છે. વધુમાં, તે તમારા સ્થાનના આધારે માહિતી પ્રદાન કરે છે. મોબાઇલ ઇન્ટરનેટ વડે વ્યક્તિગત ચેતવણીઓ મળી શકે છે. જો યુઝર રસ્તા પર ખોવાઈ જાય છે, તો મોબાઈલ ઈન્ટરનેટ તેમને ઘરનો રસ્તો શોધવામાં મદદ કરશે.

(2) સામાજિક નેટવર્કનો ઉપયોગ કરો – આજકાલ, ઘણા લોકો ફેસબુક, ઈન્સ્ટગ્રામ અને ટ્વિટર જેવી સોશિયલ નેટવર્કિંગ સાઇટ્સનો ઉપયોગ કરી રહ્યા છે. યુઝર્સ મિત્રો સાથે વોટ્સએપ અને સોશિયલ સાઇટ્સ દ્વારા સંપર્ક કરી શકે છે. બટનના સ્પર્શથી, યુઝર્સ પોતનું સામાજિક વર્તુળને ગોઠવી શકે છે.

મોબાઈલ ઈન્ટરનેટ પૈસા મેનેજ કરવામાં મદદ કરી શકે છે. યુઝર્સ એના દ્વારા યુટિલિટી બિલ ચૂકવી શકે છે, ઈન્ટરનેટ સન્ક્રિપ્શન્સ રિન્યૂ કરી શકે છે અને નવા સોદા મેળવી શકે છે. ઓનલાઈન બેંકિંગ પણ ઈન્ટરનેટના મધ્યમ દ્વારા સરળ રીતે મેનેજ કરી શકાય છે.

(3) 4G મોબાઇલ નેટવકર્સ - સેલ્યુલર નેટવકર્સ નવીનતમ મોબાઇલ નેટવકર્સનો ઉપયોગ કરવાની મંજૂરી આપે છે, જેમ કે 3G, 4G અને આગામી 5G, 4G નેટવર્ક સાથે, યુઝર્સ Wi–Fi અને હોટસ્પોટ્સ કરતાં વધુ સારું કવરેજ મેળવી શકે છે. આ નેટવકર્સ સંપૂર્ણ સુરક્ષા, સલામતી અને ગોપનીયતા પ્રદાન કરે છે.

- **મોબાઈલ ઈન્ટરનેટના ગેરફાયદા** - ઘણા ફાયદાઓ સાથે, તમે મોબાઈલ ઈન્ટરનેટ અને 4G નેટવર્ક સાથે સંકળાયેલા કેટલાક ગેરફાયદાને અવગણી શકતા નથી.

(1) ગોપનીયતાના મુદ્દાઓ - ઈન્ટરનેટ કનેકશન સાથે ગોપનીયતાની સમસ્યાઓ સામાન્ય

છે, અસંખ્ય લોકો તેમના મોબાઇલ ઉપકરણો દ્વારા ઇન્ટરનેટનો ઉપયોગ કરે છે, તેથી સર્ચ એન્જિન વારંવાર વપરાશકર્તાઓના શોધ ઈતિહાસને આર્કાઈવ કરે છે. કેટલીક કંપનીઓ તેમના અંગત લાભ માટે આ માહિતી મેળવી શકે છે.

(2) 4G નેટવર્કના ગેરફાયદા - 4G નેટવર્કની કનેક્ટિવિટી ચોક્કસ પ્રદેશો અને કેરિયર્સ સુધી મર્યાદિત છે. આ નેટવર્કનો ઉપયોગ કરવા માટે તમારી પાસે સુસંગત હાર્ડવેર હોવું આવશ્યક છે. આ નેટવર્ક ચોક્કસ સાધનો માટે સસ્તા દરે ઉપલબ્ધ છે. 4G નેટવર્કનો લાભ મેળવવા માટે યુઝર્સે આ સાધન ખરીદવું પડે છે.

મોબાઇલ તથા ઇન્ટરનેટ તેના યોગ્ય કે અયોગ્ય ઉપયોગથી જ સારું કે ખરાબ સબિત થતું હોય છે.

- **સારાંશ**

ભારત સરકારે મોબાઈલ ક્ષેત્રમાં વિવિધ કાયદાઓ અને નિયમો બનાવ્યા છે. આ કાયદાઓમાં ટેલિકોમ નિયમન અધિનિયમ, માહિતી ટેક્નોલોજી અધિનિયમ અને વ્યક્તિગત ડેટા સુરક્ષા બિલ જેવા મહત્ત્વના કાયદાઓનો સમાવેશ થાય છે. આ કાયદાઓમાં મોબાઈલ કંપનીઓ, સેવા પ્રદાતાઓ અને વપરાશકર્તાઓ બંનેને લાગુ પડે છે.

જોકે, આ કાયદાઓ હોવા છતાં, સાયબર ગુનાઓમાં વધારો થવાનું કારણ એ છે કે ટેક્નોલોજી ખૂબ જ ઝડપથી બદલાઈ રહી છે અને કાયદાઓને આ બદલાવો સાથે તાલમેલ બેસાડવામાં થોડો સમય લાગી શકે છે. આ ઉપરાંત, સાયબર ગુનેગારો પણ નવી-નવી તકનીકોનો ઉપયોગ કરીને કાયદાને ચકામણ આપવાનો પ્રયાસ કરે છે.

આ પરિસ્થિતિમાં, મોબાઈ કાયદાઓને સતત અપડેટ કરવા અને તેમની અસરકારક અમલવારી સુનિશ્ચિત કરવી જરૂરી છે. આ ઉપરાંત, નાગરિકોને સાયબર સુરક્ષા અંગે જાગૃત કરવા અને તેમને સાયબર ગુનાઓથી બચાવવા માટે શિક્ષિત કરવા પણ જરૂરી છે.

નિષ્કર્ષમાં, ભારતમાં મોબાઈલ કાયદાઓ એક જટિલ અને સતત વિકસિત થતું ક્ષેત્ર છે. આ કાયદાઓનો ઉદ્દેશ્ય નાગરિકોની ડિજિટલ સુરક્ષા સુનિશ્ચિત કરવાનો છે, પરંતુ તેમને અસરકારક રીતે અમલમાં મૂકવા માટે સતત પ્રયાસો કરવા જરૂરી છે. સાયબર ગુનાઓનો સામનો કરવા માટે, સરકાર, કાયદા અમલીકરણ એજન્સીઓ, ટેક કંપનીઓ અને નાગરિકોએ સંયુક્ત પ્રયાસો કરવા જરૂરી છે.

2.6 તમારી પ્રગતિ ચકાસો.

1. સાઇબર અપરાધ વિશે ઉદાહરણ આપી સમજાવો.

2. મેડવેર વિશે સમજાવો.

3. શું વાહન ચલાવતી વખતે મોબાઈલ ફોનનો ઉપયોગ કરવો કાયદાકીય રીતે ગુનો બને છે ?

____

____

____

4. IT Act 2000 કઈ રીતે મોબાઈલ ને લગતા સાઈબર અપરાધ ને આવરી લે છે ?

____

____

____

2.7 ચાવીરૂપ શબ્દો

1. **ભારતીય આઈ.ટી. એક્ટ :** ઈલેક્ટ્રોનિક ડેટાના માધ્યમથી કરવામાં આવતા વ્યવહારો માટે કાનૂની માન્યતા પ્રદાન કરવા માટેનો કાયદો.
2. **GPS (ગ્લોબલ પોઝિશનિંગ સિસ્ટમ) :** એક સિસ્ટમ કે જેના દ્વારા ઉપગ્રહોમાંથી કોઈ ખાસ ઉપકરણ પર સંકેતો મોકલવામાં આવે છે, જેનો ઉપયોગ પૃથ્વીની સપાટી પર ઉપકરણની સ્થિતિ બતાવવા માટે થાય છે.
3. **WiFi :** વાયરલેસ નેટવર્કિંગ ટેક્નોલોજી કે જે મોબાઈ ઉપકરણો, કમ્પ્યૂટર્સ અને અન્ય સાધનોને ઈન્ટરનેટ સાથે ઈન્ટરફેસ કરવાની મંજૂરી આપે છે.

2.8 સંદર્ભસૂચિ

1. Mobile Law in India by Pavan Duggal
2. https://www.meity.gov.in/content/information-technology-act-2000-0

એકમ-3 ઈન્ટરનેટ બેંકિંગ

: રૂપરેખા :

3.0 ઉદ્દેશ

3.1 ઈન્ટરનેટ બેંકિંગનો ઈતિહાસ

3.2 ઈન્ટરનેટ બેંકિંગની વ્યાખ્યા

3.3 ઈન્ટરનેટ બેંકિંગના પ્રકાર

3.4 ઈન્ટરનેટ બેંકિંગ વિતરણ ચેનલો

3.5 ઈન્ટરનેટ બેંકિંગ કાર્ય

3.6 ઈન્ટરનેટ બેંકિંગના ફાયદા - ગેરફાયદા

3.7 ઈન્ટરનેટ બેંકિંગ જોખમો અને પડકારો

- **સારાંશ**

3.8 તમારી પ્રગતિ ચકાસો

3.8 ચાવીરૂપ શબ્દો

3.10 સંદર્ભ સૂચિ

3.0 ઉદ્દેશ

વિદ્યાર્થીમિત્રો, આ પ્રકરણનો અભ્યાસ કર્યા બાદ તમે;

- ઈન્ટરનેટ બેંકિંગ અને તેની ઉપયોગિતા અંગે સમજણ પ્રાપ્ત કરીશો.
- ઈન્ટરનેટ બેંકિંગના પ્રકારો અને તેની સેવાઓ વિશે માહિતી મેળવશો.
- ઈન્ટરનેટ બેંકિંગની કાર્યપ્રણાલી વિશે તથા તેના ફાયદા અને ગેરફાયદા વિશે જાણીશો.
- ઈન્ટરનેટ બેંકિંગ સુરક્ષા વિશે જાણીશો.

3.1 ઈન્ટરનેટ બેંકિંગનો ઈતિહાસ

ઈન્ટરનેટ બેંકિંગની શરૂઆત 1980ના દાયકામાં થઈ. આ પહેલા ગ્રાહકોએ પોતાના બેંક એકાઉન્ટના સંચાલન માટે બેંકની સર્વિસ શાખા સુધી જવું પડતું હતું. આ ખૂબ જ સમય માંગી લે તેવું કામ હતું, સમયનો અભાવ હોય તો બેંકને લગતા કામકાજો થઈ શકતા ન હતા. 1981માં ટેલિફોન લાઇન થકી બેન્ક એકાઉન્ટ કોમ્પ્યૂટર ટીવી સ્ક્રીન સાથે જોડાયા. આ ફક્ત શરૂઆત હતી અને એ સમયે ઉપયોગ સીમિત હતો. ન્યૂયોર્કની અમુક જ બેંકો જેમકે સિટી બેંક, ચેઝ મેનહટન બેંક અને કેમિકલ બેંક આ સેવાઓ ઉપલબ્ધ કરાવતા હતા.

1990ના દાયકામાં ઈન્ટરનેટના બહોળા પ્રસારના લીધે આ સેવા ટેલીફોન લાઈનથી ઈન્ટરનેટ માધ્યમ પર આવી ગઈ. સ્ટેનફોર્ડ ફેડરલ ક્રેડિટ યુનિયન પહેલી એવી નાણાકીય સંસ્થા હતી જેણે ઈન્ટરનેટ બેંકિંગ સેવાની શરૂઆત કરી. આ એક મહત્ત્વનું પગલું હતું જેના થકી ઈન્ટરનેટ બેંકિંગનો ખૂબ પ્રચાર અને પ્રસાર થવાનો હતો. પ્રેસિડેન્શિયલ બેંક

પહેલી એવી સંસ્થા હતી જેણે તેના તમામ ગ્રાહકોને માટે ઈન્ટરનેટ બેંકિંગ સેવા શરૂ કરી. આ શરૂઆત આવનારા સમયમાં કદી પાછી ન વાળી શકાય એવી ક્રાંતિની નિમિત્ત બની રહી. 1996 માં નેટ બેંકની સ્થાપના થઈ જે પોતાના ગ્રાહકોને તમામ સેવાઓ ઓનલાઈન જ આપતી હતી તેની કોઈ સર્વિસ શાખા ન હતી. નેટ બેંકની સ્થાપનાએ સર્વિસ શાખાઓની જરૂરિયાતને મૂળભૂત રીતે બદલી નાખી. હવે બેંક એકાઉન્ટને લગતા કામકાજ માટે બેંકોની શાખા ઉપરનું અવલંબન સાવ ઘટી ગયું હતું. નેટ બેંક પછી એવી ઘણી બેન્કો બની કે જેઓ તેમની તમામ સેવાઓ ઓનલાઈન જ ઉપલબ્ધ કરાવતી હતી. આવી તમામ બેંકોની સેવાઓ એકંદરે બીજી બધી ટ્રેડિશનલ બેંકો કરતા સસ્તી તથા ઉપયોગ માટે સરળ હતી.

2000ના દાયકામાં ઈન્ટરનેટ બેંકિંગ એક સ્થાપિત ધોરણ બની ચૂક્યું હતું. જેના પરિણામે લગભગ 80 ટકાથી વધુ બેંકો ઈન્ટરનેટ બેંકિંગની સેવાઓ શરૂ કરી ચૂકી હતી. બે દાયકા પહેલાં આવું કંઈક બનવું સાવ અશક્ય લાગી રહ્યું હતું પણ હવે એ નક્કર હકીકત બની ચૂકી હતી. ઈન્ટરનેટ બેંકિંગનો વ્યાપ ત્યારબાદ વધતો જ રહ્યો પરિણામે બેંકોને લગતા તમામ કાર્યો તથા સેવાઓ ઓનલાઈન જ ઉપલબ્ધ થઈ ચૂકી હતી.

આજના સમયમાં ગ્રાહકો પોતાના બેન્ક એકાઉન્ટનું સંચાલન કોઈપણ ડિજિટલ ઉપકરણ દ્વારા વિશ્વના કોઈપણ ખૂણેથી અને કોઈપણ સમયે કરવામાં સક્ષમ છે.

3.2 ઈન્ટરનેટ બેંકિંગની વ્યાખ્યા

ઈન્ટરનેટ બેંકિંગ, કે જેને નેટ બેંકિંગ તરીકે પણ ઓળખવામાં આવે છે, તે ઈન્ટરનેટના માધ્યમથી બેંકિંગ વ્યવહારો કરવા માટેની ડિજિટલ પદ્ધતિ છે. તે એક ઈલેક્ટ્રોનિક સિસ્ટમ છે, જેને બેંક એકાઉન્ટ ધરાવનાર કોઈપણ વ્યક્તિ સક્રિય કરી શકે છે અને તેનો ઉપયોગ તેમની નાણાકીય કાર્યો માટે કરી શકે છે.

પહેલા ભૌતિક રીતે કરવામાં આવતા બેંકિંગના મોટાભાગના કાર્યો ઈન્ટરનેટ બેંકિંગ દ્વારા હાથ ધરવામાં આવી શકે છે. ઈન્ટરનેટ બેંકિંગ સેવાનો લાભ લેવા માટે આપણે કોઈપણ ડિજિટલ ગેજેટ જેમાં ઈન્ટરનેટ કનેક્ટિવિટી હોય એનો ઉપયોગ કરી શકીએ છીએ.

ઓનલાઈન બેંકિંગનો ઉપયોગ કોઈપણ કોમ્પ્યૂટર દ્વારા કરવા માટે ઈન્ટરનેટ એક્સપ્લોરર થકી જે તે બેંકની ઈન્ટરનેટ બેંકિંગ માટેની વેબસાઈટ પર જઈને ગ્રાહકને બેંક દ્વારા આપવામાં આવેલ યુઝરનેમ તથા પાસવર્ડ વડે લોગિન કરવાનું રહે છે. લોગીન થઈ ગયા બાદ ગ્રાહક જે તે મેનુમાં જઈને ત્યાં આપેલ સર્વિસનો ઉપયોગ કરી શકે છે. મોબાઈલ દ્વારા ઈન્ટરનેટ બેંકિંગ ઈન્ટરનેટ એક્સપ્લોરર અથવા ઈન્ટરનેટ બેંકિંગની એપ દ્વારા બેંકિંગ સુવિધા નો લાભ લઈ શકાય છે. આના આપણે માટે બેંક દ્વારા અધિકૃત એપ મોબાઈલમાં ડાઉનલોડ કરવાની રહે છે. અનઅધિકૃત એપ દ્વારા ઈન્ટરનેટ બેંકિંગ શક્ય નથી.

3.3 ઈન્ટરનેટ બેંકિંગના પ્રકારો

માહિતીપ્રદ ઈન્ટરનેટ બેંકિંગ (Informational Internet Banking)

ઈન્ફોર્મેશનલ ઈન્ટરનેટ બેંકિંગનો સીધો અર્થ છે કે બેન્ક તેના ઉત્પાદનો અને સેવાઓ વિશેની મૂળભૂત માહિતી પોતાના ગ્રાહકો સુધી પહોંચાડે છે. આ સેવા મુખ્યત્વે માત્ર માર્કેટિંગ હેતુઓ માટે જ હોય છે, અને તેનું બેંકની મુખ્ય કાર્ય પ્રણાલી સાથે કોઈ પ્રકારનું જોડાણ હોતું નથી. બેંકિંગનો આ પ્રકાર બેંક ગ્રાહકોને ખાતા જોવા અથવા જાળવવાની મંજૂરી આપતું નથી, ન તો તે નાણાકીય સંસ્થા અને ગ્રાહકો વચ્ચે સંચાર કરવાની મંજૂરી આપે છે.

કોમ્યુનિકેટિવ ઓનલાઈન બેંકિંગ (Communicative Online Banking)

કોમ્યુનિકેટિવ ઓનલાઈન બેંકિંગ ગ્રાહકો અને બેંક વચ્ચે કેટલાક સંચાર માટેની પરવાનગી આપે છે. જો કે, આ સામાન્ય રીતે એકાઉન્ટની પૂછપરછ, નવા એકાઉન્ટ અપડેટ્સ, લોન અથવા મોર્ટગેજ એપ્લિકેશન્સ, સંપર્ક માહિતી અપડેટ્સ અને બેલેન્સ જાણવા જેવી મૂળભૂત ક્રિયા-પ્રતિક્રિયાઓ સુધી મર્યાદિત છે. કોમ્યુનિકેટિવ ઓનલાઈન બેંકિંગ બેંકની મુખ્ય કમ્પ્યૂટર સિસ્ટમ સાથે જોડાયેલી હોય છે.

ટ્રાન્ઝેકશનલ ઈન્ટરનેટ બેંકિંગ (Transactional Internet Banking)

ટ્રાન્ઝેકશનલ ઈન્ટરનેટ બેંકિંગ જે સૌથી વધુ લોકપ્રિય ઓનલાઈન બેંકિંગ પ્રકાર છે, તે પરંપરાગત સંસ્થાના તમામ લાભો ઑનલાઇન પ્રદાન કરે છે. આમાં ગ્રાહકનો પોતાના બેંક એકાઉન્ટ્સ પર સંપૂર્ણ નિયંત્રણ શામેલ છે. જમા, ઉપાડ, ટ્રાન્સફર, અપડેટ્સ અને ઑનલાઇન ચૂકવણી. સુરક્ષાના વધારાના પગલાં હવે ઈન્ટરનેટ બેંકિંગને સુરક્ષિત બનાવે છે. ટૅક્નોલૉજીના વ્યાપના લીધે આ પ્રકારની સુવિધા ગ્રાહકો માટે ખૂબ અનુકૂળ બની રહી છે.

3.4 ઈન્ટરનેટ બેંકિંગ વિતરણ ચેનલો

ઈન્ટરનેટ બેંકિંગ દ્વારા નીચે જણાવેલી વિવિધ સેવાઓ ઉપલબ્ધ હોય છે. નીચે જણાવેલ સેવાઓ મુખ્ય સેવાઓ તરીકે ઓળખાય છે. આ સેવાઓ ઉપરાંત પણ વિવિધ પ્રકારની સેવાઓ ઈન્ટરનેટ બેંકિંગના માધ્યમથી ઉપલબ્ધ થતી હોય છે. આ પૈકી મુખ્ય સેવાઓની વિસ્તૃત જાણકારી નીચે આપેલ છે.

ખાતાની માહિતી : ખાતાની માહિતીમાં મુખ્યત્વે ખાતાધારકોના નામ, ખાતાનું બેલેન્સ, પ્રકાર, લઘુતમ જમા રાશી (મિનિમમ બેલેન્સ) વગેરે વિગતો સામેલ હોય છે. ગ્રાહકો પોતે પણ વિવિધ પ્રકારના ખાતાઓ જેમ કે સેવિંગ ખાતુ અથવા ડિપોઝિટ ખાતું ઓનલાઈન જ ખોલાવી અથવા બંધ કરાવી શકે છે.

લેવડદેવડ : ખાતાની લેવડદેવડમાં મુખ્યત્વે ખાતામાંથી જમા તથા ઉપાડ વિશેની સેવાઓ આવે છે. આ અંતર્ગત ગ્રાહકો પોતાના એક ખાતામાંથી પોતાના બીજા ખાતામાં અથવા બીજા ગ્રાહકના ખાતામાં પૈસા મોકલી કરી શકે છે. ગ્રાહકો પોતાના ખાતામાંથી બિલ પેમેન્ટ પણ કરી શકે છે.

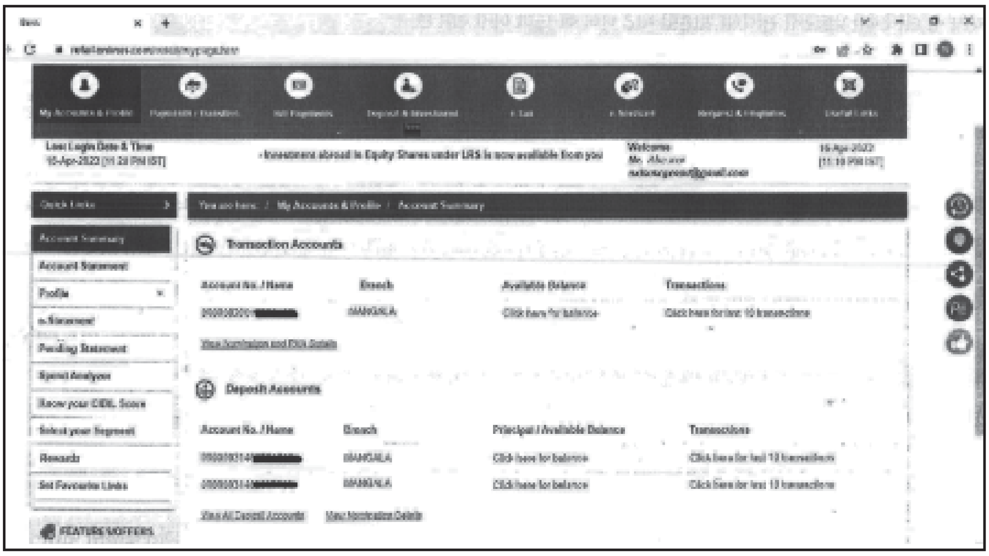
ખાતાની લેવડદેવડ નીચે જણાવેલ ત્રણ પ્રકારે થઈ શકે છે.

1. **NEFT (National Electronic Funds Transfer)** - આ એક ઈન્ટરબેંક ઈલેક્ટ્રોનિક ફંડ ટ્રાન્સફર સુવિધા છે. આ સુવિધામાં બેંકો વચ્ચે દર એક કલાકે બેચ દ્વારા તમામ વ્યવહારો મંજૂર કરવામાં આવે છે. NEFT ફંડ ટ્રાન્સફર 1–2 કલાકની અંદર થાય છે. આ અંતર્ગત ટ્રાન્સફર માટે કોઈ મહત્તમ અને લઘુત્તમ રકમ નિર્ધારિત નથી. આ સુવિધા તમામ સ્થાનિક બેંકોની શાખાઓમાં ઉપલબ્ધ હોય છે. બેંકના કામકાજના દિવસોમાં સોમવારથી શુક્રવાર સવારે 8 થી સાંજના 6:30 વાગ્યા સુધી અને કામકાજના શનિવારે સવારે 8 થી બપોરે 1 વાગ્યા સુધી ઉપલબ્ધ છે.

2. **RTGS (Real-Time Gross Settlement)** આ પણ એક ઈન્ટરબેંક ઈલેક્ટ્રોનિક ફંડ ટ્રાન્સફર સુવિધા છે, દરેક ટ્રાન્ઝેકશનના આધારે બેંકો વચ્ચે એકાઉન્ટ સેટલ કરવામાં આવે છે. આ સુવિધા દ્વારા રિઅલ-ટાઈમ, એટલે કે ગણતરીની ક્ષણોમાં જ બેંક એકાઉન્ટ વચ્ચે ફંડ ટ્રાન્સફર થઈ શકે છે. આ સુવિધા ફક્ત RTGS સક્ષમ

શાખાઓ દ્વારા જ ઓફર કરી શકાય છે, બેંકના કામકાજના દિવસોમાં સવારે 8 થી સાંજના 4 વાગ્યાની વચ્ચે ઉપયોગ માટે ઉપલબ્ધ છે.

3. **IMPS (Immediate Mobile Payment Services)** મોબાઈલ ફોન દ્વારા ઈલેક્ટ્રોનિક ફંડ ટ્રાન્સફર સુવિધા જે ઈન્ટર-બેંક અને ઈન્ટ્રા-બેંક ટ્રાન્સફરની મંજૂરી આપે છે. મોબાઈલ બેંકિંગ સુવિધા આવશ્યક છે. તેનો ઉપયોગ એટીએમ અને ઈન્ટરનેટ બેંકિંગ દ્વારા પણ થઈ શકે છે. IMPS ટ્રાન્સફર ત્વરિત થાય છે. ન્યૂનતમ ટ્રાન્સફર પર કોઈ મર્યાદા નથી. મહત્તમ મર્યાદા વિવિધ બેંકો દ્વારા નિર્ધારિત છે. આ સુવિધા બેંક રજાઓ સહિત સમગ્ર વર્ષ દરમિયાન 24*7 (24 કલાક અને 7 દિવસ) ઉપલબ્ધ છે.



આકૃતિ #1 : ઈન્ટરનેટ બેંકિંગ વેબસાઈટનું હોમ પેજ

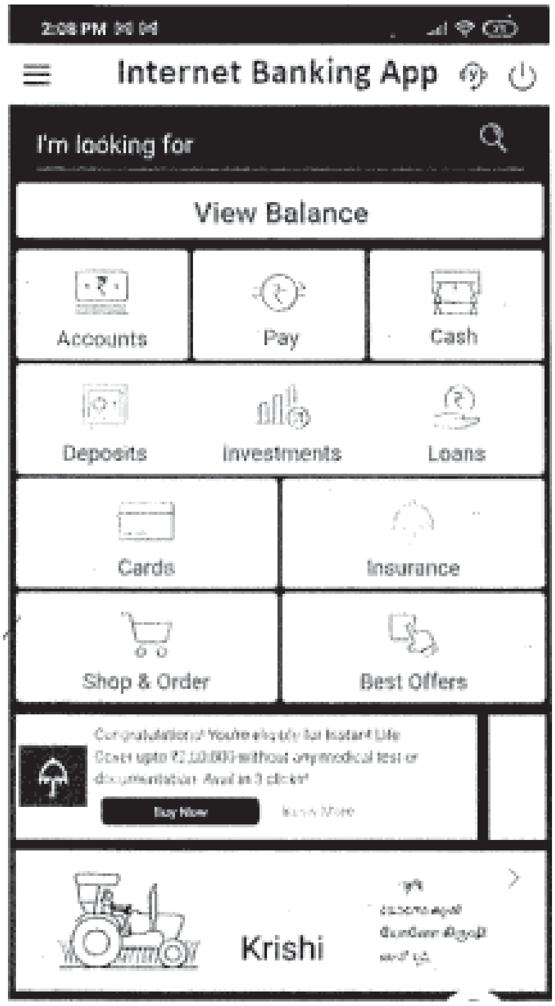
મુખ્ય બેંક સુવિધાઓ :

(1) લોન : ગ્રાહકો ઈન્ટરનેટ બેંકિંગના માધ્યમથી લોન માટેની અરજી પણ કરી શકે છે. વિવિધ પ્રકારની લોન જેમાં હોમ લોન, વાહન લોન, કૃષિ લોન, બિઝનેસ લોન, પર્સનલ લોન, એજયુકેશન લોન, ગોલ્ડ લોન વગેરેનો સમાવેશ થાય છે, તે માટેની અરજી ઑનલાઇન થઈ શકે છે. ગ્રાહકો તેમની લોનની જરૂરિયાત પ્રમાણે માહિતી ભરીને તથા જરૂરી પુરાવો અપલોડ કરીને લોન માટે અરજી કરી શકે છે.

(2) ડેબિટ ક્રેડિટ કાર્ડ સંબંધિત સેવાઓ : ગ્રાહકો તેઓના ક્રેડિટ/ ડેબિટ કાર્ડની લગતી સેવાઓ જેમ કે કાર્ડનો પીન સેટ કે રીસેટ કરવો, નવા કાર્ડની માંગણી, જૂના કાર્ડ બ્લોક કરવા, કાર્ડને અલગ અલગ રીતે ઉપયોગ કરવા માટેની લિમિટ સેટ કરવી વગેરે કાર્યો કરી શકે છે.

(3) પ્રોફાઈલ મેનેજમેન્ટ : ગ્રાહકો પ્રોફાઈલ મેનેજમેન્ટ અંતર્ગત પોતાની વિગતો જેમ કે મોબાઈલ નંબર ઈ-મેઈલ આઈડી, કાયમી તથા હાલનું સરનામું, વગેરે બદલી શકે છે. ખાતાની લેવડદેવડ માટે જરૂરી જે તે ખાતાના નંબર ગ્રાહકનું નામ તથા ખાતુ જે બેંકમાં હોય તે બેન્કનો કોડ નંબર ઉમેરી કે બદલી શકે છે.

(4) ઈન્વેસ્ટમેન્ટ : ઈન્ટરનેટ બેંકિંગ એકાઉન્ટનો ઉપયોગ કરીને રોકાણ કરી શકાય છે પણ જો બેંક મ્યુચ્યુઅલ ફંડ દ્વારા સૂચિબદ્ધ હોય તો, રોકાણકારો તેમના મ્યુચ્યુઅલ ફંડ સાથે લોગ–ઈન અને પાસવર્ડ બનાવી શકે છે અથવા ફંડમાં સીધું રોકાણ કરવા માટે તેમના



હાલના ફોલિયો નંબરનો ઉપયોગ કરી શકે છે. આવા રોકાણો માટે ફોર્મ ભરવાની અથવા એપ્રુવલ પ્રક્રિયાની ઔપચારિકતાની જરૂર પડતી નથી કારણ કે નાણાં સીધા ફંડમાં ટ્રાન્સફર થાય છે અને રોકાણકારને એકમો ફાળવવામાં આવે છે. રિડેમ્પશન વિનંતીઓના પરિણામે મળતા પૈસા પણ સીધા બેંક ખાતામાં જમા થાય છે. રોકાણકારોને ફોર્મ ભરવાની ઝંઝટ વિના બચત ખાતામાં કોઈપણ વધારાની રકમ ઝડપથી જમા કરાવવા માટે આ સુવિધા ખૂબ જ ઉપયોગી છે.

(5) ઈન્સ્યોરન્સ : જેમ ગ્રાહકો બધી જરૂરી વસ્તુઓ ખરીદે છે અને યુટિલિટી બિલ્સ ઓનલાઈન ચૂકવે છે, તેવી જ રીતે ઈન્સ્યોરન્સ ઓનલાઈન ખરીદવું શક્ય છે. જો કે, ખરીદી માટે આગળ વધતા પહેલા બેંકના ગ્રાહકોએ પોલિસીના ફાયદાઓ તપાસવા જોઈએ અને અન્ય સમાન પોલિસીઓ સાથે તેની તુલના કરવી જોઈએ.

(6) ઉત્પાદનો / નીતિઓની માહિતી : બેંકો સમયાંતરે તેઓની સેવાઓમાં વિવિધ પ્રકારના સુધારા-વધારા કરતા રહે છે. આ સિવાય, નીતિનિયમો માં પણ સમયાંતરે ફેરફાર થતા હોય છે. આ તમામ પ્રકારની માહિતી પણ ઈન્ટરનેટ બેંકિંગના માધ્યમથી ગ્રાહકો સુધી ખૂબ જ સરળતાથી પહોંચાડી શકાય છે.

(7) વિનંતીઓ અને પૂછપરછ : ઈન્ટરનેટ બેંકિંગ દ્વારા વિવિધ પ્રકારની વિનંતીઓ અને પૂછપરછ ગણતરીની પળોમાં શક્ય બને છે. કટોકટી (ઇમર્જન્સી) ની પરિસ્થિતિ માટેની વિનંતીઓ જેમ કે એટીએમ કે ડેબિટ કાર્ડ બ્લોક કરવા, SMS એલર્ટ શરૂ કરવા, ચેક પેમેન્ટ રોકવું, વગેરે ખૂબ જ સરળતાથી અને કોઈપણ સ્થળેથી તરત જ શક્ય બને છે. આ સિવાય પણ નીચે દર્શાવેલ વિનંતીઓ તથા પૂછપરછ ઈન્ટરનેટ બેંકિંગ દ્વારા સરળતાથી થઈ શકે છે.

1. પ્રોફાઈલની વિગતો ઉમેરવી અથવા બદલવી
2. પોતાનો લોગીન/પ્રોફાઈલ/ટ્રાન્જેકશન પાસવર્ડ બદલવો
3. નવી ચેકબુક ઈશ્યુ કરવા માટે વિનંતી કરવી
4. નવો એટીએમ/ડેબિટ/ક્રેડિટ કાર્ડ ઈશ્યુ કરાવવા
5. એકાઉન્ટનું સ્ટેટમેન્ટ માટેની વિનંતી
6. ઓનલાઈન શૉપિંગ માટેની મહત્તમ ટ્રાન્જેકશન લિમિટ સેટ કરવી
7. ફંડ ટ્રાન્સફર માટે લાભાર્થી (beneficiary)ની વિગતો ઉમેરવી અથવા બદલવી

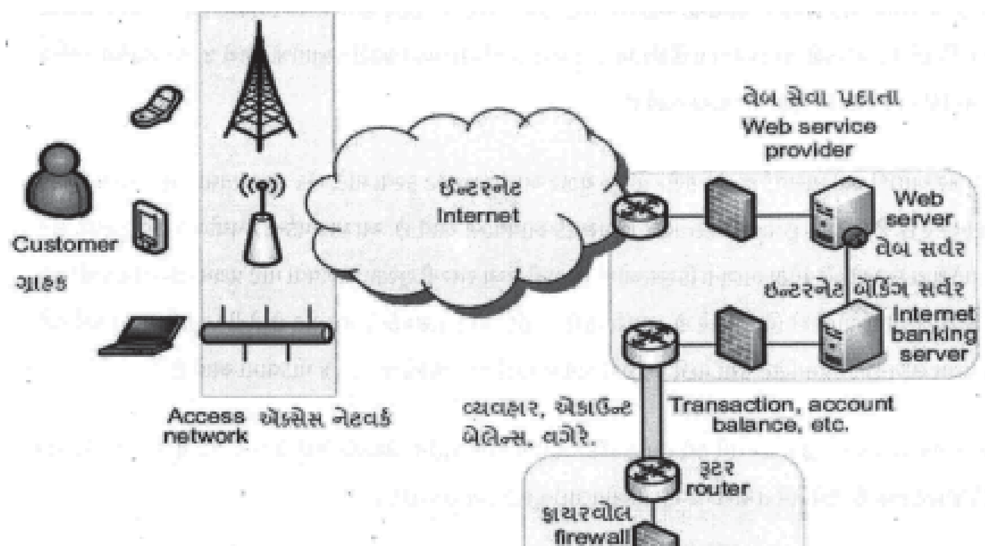
(8) સ્થાયી સૂચનાઓ : આ એક વિશિષ્ટ પ્રકારની સેવા છે જેના થકી ગ્રાહકો સમયાંતરે નિયમિત કરવાના એવા લેવડદેવડના કાર્યો જેવા કે બિલ પેમેન્ટ, જે તે ખાતામાં પૈસા જમા કરવા વગેરેને લગતી સૂચનાઓ ઉમેરી શકે છે. એક વાર જરૂરી સૂચનાઓ ઉમેરી અને એનો અમલ કયારે કયારે કરવાનો રહેશે તેને લગતી સૂચનાઓ ઉમેરી દીધા બાદ તે આપોઆપ જ તેના સમયે થતી રહેતી હોય છે. આ સુવિધાના લીધે ગ્રાહકે વારંવાર એક જ પ્રકારના કામ કરતા રહેવાની તથા તેને યાદ રાખવાની જરૂર રહેતી નથી.

3.5 ઈન્ટરનેટ બેંકિંગ કાર્ય

કાર્યપ્રણાલી વિશે આપણે બે પ્રકારે જાણીશું, પહેલું એની તકનીકી કાર્યપ્રણાલી તથા નેટબેંકિંગનો ઉપયોગ કરવા માટે જરૂરી મુદ્દાઓ.

તકનીકી કાર્યપ્રણાલી

ઈન્ટરનેટ બેંકિંગ સેવા મુખ્યત્વે ઈન્ટરનેટના માધ્યમ દ્વારા પૂરી પાડવામાં આવે છે. દરેક બેંકો કે જે ઈન્ટરનેટ બેંકિંગની સુવિધા ઉપલબ્ધ કરાવે છે તે બેંકોનો તમામ ડેટા (ગ્રાહક તથા ખાતા વિશેની માહિતી) ઈન્ટરનેટ બેંકિંગ સર્વર (ઈન્ટરનેટના માધ્યમથી જોડાયેલી કમ્પ્યૂટર સિસ્ટમ) પર ઉપલબ્ધ હોય છે. નીચે આપેલ આકૃતિ નંબર 3, ઈન્ટરનેટ બેંકિંગ સિસ્ટમના વિવિધ એકમો એકબીજા સાથે કઈ રીતે જોડાયેલા હોય છે એ દર્શાવે છે.



આકૃતિ #3 : ઈન્ટરનેટ બેંકિંગ સિસ્ટમના એકમો

આ સર્વર એક તરફ વેબ સર્વર સાથે અને બીજી તરફ તે બેંકના આંતરિક નેટવર્ક સાથે જોડાયેલું હોય છે. ગ્રાહકો એકસેસ નેટવર્ક દ્વારા ઈન્ટરનેટ સાથે જોડાયેલા હોય છે. તેઓ ઈન્ટરનેટ એક્સપ્લોરર દ્વારા બેંકની વેબસાઈટ પર અથવા બેંકની ઈન્ટરનેટ બેંકિંગ એપ્લિકેશન પોતાના મોબાઈલમાં ઈન્સ્ટોલ કરીને પોતાના એકાઉન્ટમાં લોગીન કરીને ઈન્ટરનેટ બેંકિંગ સેવાનો લાભ થઈ શકે છે.

નેટબેંકિંગ ખાતું એ બેંક ખાતાનું ડિજિટલ એકસ્ટેશન છે, નેટબેંકિંગ ખાતું ખોલવા માટે, ગ્રાહકે ડિજિટલ પાસવર્ડ જનરેટ કરવાની જરૂર છે જે તમને ઈન્ટરનેટ પર વ્યવહાર કરવા સક્ષમ બનાવે છે.

નેટબેંકિંગ ખાતું ખોલવા માટે, ગ્રાહકે આ ચાર પગલાંને અનુસરવાની જરૂર છેઃ

1. નેટબેંકિંગ એકાઉન્ટ માટે તમારી બેંકનો સંપર્ક કરો - નેટબેંકિંગ એકાઉન્ટ શરૂ કરવા માટેનું તમારું પ્રથમ પગલું એ છે કે તમારા વર્તમાન બેંક ખાતા માટે ઓનલાઈન બેંકિંગ સુવિધાને સક્ષમ કરવા માટે બેંકનો સંપર્ક કરવો. જ્યાં સુધી તમે તમારી બેંકને તમારી બેંકિંગ સેવાઓ ઓનલાઈન શરૂ કરવા માટે વિનંતી ન કરો ત્યાં સુધી, તમે આ સેવાઓનો ઉપયોગ કરવાનું શરૂ કરી શકતા નથી. તમને ઈન્ટરનેટ બેંકિંગ દ્વારા ડિજીટલ ટ્રાન્ઝેકશન કરવા સક્ષમ બનાવવા માટે ઉચ્ચ સુરક્ષા જાળવવામાં આવે છે. તમારે તમારી બેંકને તમારા ખાતા માટે નેટબેંકિંગ શરૂ કરવાનો તમારો હેતુ જણાવવો જોઈએ. બેંક તમારી વિનંતી પ્રાપ્ત કર્યા બાદ, તે તમને બે મુખ્ય કોડ પ્રદાન કરે છે જે તમને તમારા એકાઉન્ટમાં ઑનલાઇન લોગ ઈન કરવામાં મદદ કરે છે.

2. તમારું યુઝર આઈડી અને પાસવર્ડ એકત્રિત કરો - નેટબેંકિંગ કામ કરે તે માટે, તમારે તમારા ઈન્ટરનેટ બેંકિંગ એકાઉન્ટમાં લોગ ઈન કરવા માટે તમારું યુઝર આઈડી અને પાસવર્ડ જાણવાની જરૂર છે. આ વપરાશકર્તા ID તમારા બેંક એકાઉન્ટ નંબરથી અલગ છે, જે તમારા બેંક ખાતાની પ્રાથમિક ઓળખ તરીકે સેવા આપે છે. તમારે તમારી બેંકને યુઝર આઈડી અને પાસવર્ડ બનાવવા વિનંતી કરવી પડશે. નવા ખાતાના કિસ્સામાં ખાતું ખોલાવતી આ વખતે જરૂરી દસ્તાવેજો સાથેજ નેટ બેંકિંગ માટેનો યુઝર આઈડી અને પાસવર્ડ પણ સોંપવામાં આવે છે.

3. નવું યુઝર આઈડી અને પાસવર્ડ જનરેટ કરો - તમારું યુઝર આઈડી જનરેટ કરવા માટે, બેંક શરૂઆતમાં તમને નંબરોનો એક સેટ પ્રદાન કરે છે જેમાં તમને છુપાવેલા દસ્તાવેજમાં પાસવર્ડ આપવામાં આવે છે. આ પાસવર્ડનો ઉપયોગ એકવાર લોગ ઈન કરવા માટે થાય છે અને બેંક મોટા ભાગના કિસ્સાઓમાં ખાતાની ઉચ્ચ સ્તરની સુરક્ષા જાળવવા માટે પ્રથમ લોગ ઈન કર્યા પછી આ પાસવર્ડ બદલવા ગ્રાહકોને વિનંતી કરે છે. તમારી પાસે આઈડી અને પાસવર્ડનો નવો સેટ છે તેની ખાતરી કરવા માટે તમે તમારા પ્રથમ લોગ–ઈનને પ્રમાણિત કર્યા પછી આઈડી અને પાસવર્ડ બદલવાની પણ ફરજ પાડવામાં આવે છે.

4. ઑનલાઈન વ્યવહારો શરૂ કરો – તમે હવે તમારા બેંક ખાતામાં ઓનલાઈન લોગ–ઈન કર્યું છે અને નવો યુઝર આઈડી અને પાસવર્ડ જનરેટ કર્યો છે. હવે તમે તમારા વ્યવહારો ઓનલાઈન શરૂ કરી શકો છો.

3.6 ઈન્ટરનેટ બેંકિંગના ફાયદા - ગેરફાયદા

★ **ફાયદા**

- ઓનલાઈન બેંકિંગની મદદથી ખાતું ખોલવું તથા તેનો ઉપયોગ કરવો સરળ હોય છે. ખાતુ ખોલવા માટે ફોર્મ પણ ઓનલાઇન ભરી શકાય છે તથા જરૂરી દસ્તાવેજ પુરાવા પણ ઓનલાઇન જ અપલોડ થઈ શકે છે, બેંક દ્વારા ફોર્મની વિગતો તથા દસ્તાવેજી પુરાવા ચકાસીને ખાતા માટેની મંજૂરી આપવાથી નવું ખાતું ખૂલી જતું હોય છે.
- તે ખૂબ અનુકૂળ છે, કારણ કે ગ્રાહક પોતાના બિલ સરળતાથી ચૂકવી શકે છે અને વિશ્વમાં લગભગ ગમે ત્યાંથી ખાતાઓ વચ્ચે ભંડોળને ટ્રાન્સફર કરી શકાય છે.
- બિલ ચૂકવ્યા બાદ બિલોની રસીદો સાચવી રાખવાની જરૂર નથી, કારણ કે હવે તમામ વ્યવહારો સરળતાથી online જ જોઈ શકો છો.
- તે દરેક સમયે ઉપલબ્ધ છે. ગ્રાહકો તેમના કાર્યો ગમે ત્યાંથી અને કોઈપણ સમયે કરી શકો છો, રાત્રે અથવા રજાના દિવસે પણ જ્યારે બેંક બંધ હોય. તેના માટે યુઝર પાસે માત્ર એક સક્રિય ઈન્ટરનેટ કનેકશન હોવું જરૂરી છે.

- તે ઝડપી અને કાર્યક્ષમ છે. ભંડોળ એક ખાતામાંથી બીજા ખાતામાં ખૂબ જ ઝડપથી ટ્રાન્સફર થાય છે. ઇન્ટરનેટ બેંકિંગ દ્વારા પણ સરળતાથી અનેક એકાઉન્ટ્સ મેનેજ કરી શકાય છે.
- ગ્રાહકો તેઓના વ્યવહારો અને એકાઉન્ટ બેલેન્સ પર હંમેશાં નજર રાખી શકે છે. ગ્રાહકો કોઈપણ કપટપૂર્ણ પ્રવૃત્તિ વિશે અથવા અનઅધિકૃત વ્યક્તિ તેઓના એકાઉન્ટને કોઈ ગંભીર નુકસાન પહોંચાડે તે પહેલાં તેના જોખમ વિશે જાણી શકે છે.
- બેંકો માટે તેમના ઉત્પાદનો અને સેવાઓને સમર્થન આપવા માટે તે એક ઉત્તમ માધ્યમ છે. વધુ ઑનલાઇન સેવાઓમાં લોન અને રોકાણ વિકલ્પોનો સમાવેશ થાય છે.

★ **ગેરફાયદા**

- ઇન્ટરનેટ બેંકિંગના ઉપયોગને સમજવું શરૂઆતના તબક્કામાં મુશ્કેલ હોઈ શકે છે. કેટલીક સાઇટ્સ એવી છે જે ઓનલાઈન એકાઉન્ટ્સ કેવી રીતે ઉપયોગ કરવા તેની વિસ્તૃત માહિતી આપે છે (બધી બેંકો આ પ્રમાણેની માહિતી પ્રદાન કરતી નથી). તેથી, જે વ્યક્તિને માટે ટૅક્નોલૉજીનો ઉપયોગ સરળ નથી તેવા વ્યક્તિને કેટલીક મુશ્કેલીનો સામનો કરવો પડી શકે છે.
- જો ગ્રાહક પાસે ઇન્ટરનેટ કનેકશન ન હોય તો તેઓ પાસે ઓનલાઈન બેંકિંગની ઍક્સેસ પણ નથી, આમ, ઇન્ટરનેટ એક્સેસની ઉપલબ્ધતા વિના, તે ઉપયોગી ન હોઈ શકે.
- વ્યવહારોની સુરક્ષા એ એક મોટો મુદ્દો છે. તમારા એકાઉન્ટની માહિતી ઇન્ટરનેટ પર અનધિકૃત લોકો દ્વારા હેક થઈ શકે છે.
- પાસવર્ડ સુરક્ષા આવશ્યક છે. પાસવર્ડ પ્રાપ્ત કર્યા પછી, તેને બદલો અને તેને યાદ રાખવો ખૂબ જ અનિવાર્ય છે. નહિતર, તમારા એકાઉન્ટનો દુરુપયોગ થઈ શકે છે. બેંકિંગ માહિતી કેટલાક ઉપકરણો પર ફેલાયેલી હોઈ શકે છે, જેનાથી તેનો અનઅધિકૃત ઉપયોગ થવાની શક્યતા રહેલી છે.
- જો બેંકનું સર્વર કાર્ય નથી કરી રહ્યું, તો એકાઉન્ટને ઍક્સેસ કરી શકાય નહીં.
- જો બેંકનું સર્વર ડાઉન હોય, નેટ કનેક્ટિવિટી ગુમાવવાને કારણે અથવા ધીમા કનેકશનને કારણે, તો તે જાણવું મુશ્કેલ હોઈ શકે છે કે તમારો વ્યવહાર થયો હતો કે નહીં.
- ગ્રાહકો માટે વધુ પડતું માર્કેટિંગ અને વધારાની સૂચનાઓ કંટાળાજનક હોઈ શકે છે. વધુમાં ગ્રાહકો સતત ઈમેઇલ્સ અને અપડેટ્સથી નારાજ થઈ શકે છે.

3.7 ઇન્ટરનેટ બેંકિંગ જોખમો અને પડકારો

ઓનલાઈન બેંકિંગ ત્યારે જ સુરક્ષિત છે જ્યારે પાછળના છેડે સુરક્ષિત બેંક ટૅક્નોલૉજી આગળના છેડે સારી રીતે માહિતગાર અને જે ચેતેલા (alert) ગ્રાહકો સાથે મળે છે. એકાઉન્ટ ધારક તરીકે, તમારા એકાઉન્ટ્સ સુરક્ષિત છે કે કેમ તેની ખાતરી કરવામાં તમારી ભૂમિકા અગત્યની છે. સામાન્ય રીતે મોટા પાયે થયેલા માહિતી ભંગને સમાચારોમાં સ્થાન મળે છે, પરંતુ ગુનેગારો ગ્રાહકો પર સીધો હુમલો કરીને નાના પાયા પર પણ કામ કરે છે.

ઇન્ટરનેટ બેંકિંગના કિસ્સામાં વ્યવહારોની સુરક્ષા ખૂબ જ મહત્ત્વપૂર્ણ છે કારણ કે આ વ્યવહારો અસુરક્ષિત ચેનલ પર થાય છે જે ઇન્ટરનેટ છે. તેથી ઇન્ટરનેટ બેંકિંગ દ્વારા થતા તમામ વ્યવહારો એનક્રિપ્ટેડ સ્વરૂપમાં થાય છે. આપણે એવા વેબપેજ દ્વારા જ વ્યવહાર કરવો જોઈએ જે આપણે જાણીએ છીએ અથવા જ્યારે તેમની સારી પ્રતિષ્ઠા હોય. તેથી,

સરળ શબ્દોમાં, તમારે તે વેબપેજની મુલાકાત લેવી જોઈએ કે જેના પર તમે વિશ્વાસ કરો છો અને ગ્રાહકો સુરક્ષિત તથા વિશ્વાસપાત્ર ગેટવે દ્વારા જ વ્યવહારો કરવાની ભલામણ કરવામાં આવે છે. આમ કરવાથી કોઈપણ ત્રીજી વ્યક્તિ તમારી કોઈપણ પ્રકારની અંગત માહિતી વિશે જાણી શકશે નહિ.

નીચે આપેલ મહત્ત્વપૂર્ણ જાણકારી ગ્રાહકના ઇન્ટરનેટ બેંકિંગના અનુભવને સુરક્ષિત અને સુખદ બનાવે છે.

★ **સુરક્ષિત ઓનલાઈન બેંકિંગ માટે મહત્વપૂર્ણ સુરક્ષા ટિપ્સ**

1. તમારા બ્રાઉઝરના એડ્રેસ બારમાં URL ટાઈપ કરીને જ તમારી બેંકની વેબસાઈટને ઍક્સેસ કરો.
2. ઓનલાઈન બેંકિંગ ઓફર કરતી મોબાઈલ એપ્લીકેશન સ્ટોર્સ (Google Playstore, Apple App Store, Blackberry App World, Ovi, Store, Windos Marketplace વગેરે) પરથી કોઈપણ અનઅધિકૃત એપ્લિકેશન ડાઉનલોડ કરવાથી સાવચેત રહો. ડાઉનલોડ કરતા પહેલા તમારી બેંકનો સંપર્ક કરીને તેમની અધિકૃતતા તપાસો.
3. સાઇટને એકસેસ કરવા માટે કોઇપણ ઈ–મેલ મેસેજની કોઈપણ લિંક પર ક્લિક કરશો નહીં.
4. તમારી અંગત માહિતી, પાસવર્ડ અથવા વન ટાઈમ એસએમએસ પાસવર્ડ મેળવવા માટે બેંક અથવા તેના કોઈપણ પ્રતિનિધિ તમને કયારેય ઈમેલ/એસએમએસ મોકલતા નથી અથવા તમને ફોન પર કૉલ કરતા નથી. આવા કોઈપણ ઈમેલ/એસએમએસ અથવા ફોન કૉલ એ ઇન્ટરનેટ બેંકિંગ દ્વારા તમારા ખાતામાંથી છેતરપિંડીથી પૈસા ઉપાડવાનો પ્રયાસ છે. આવા ઈમેલ/એસએમએસ કે ફોન કૉલનો કયારેય જવાબ આપશો નહીં. જો તમને આવો કોઈ ઈ–મેલ/એસએમએસ અથવા ફોન કૉલ મળે તો કૃપા કરીને આના વિષે બેંકની વેબસાઈટ અથવા ટેલિફોન નંબર પર તરત જ જાણ કરો.
5. જો તમે આકસ્મિક રીતે તમારા ઓળખપત્રો જાહેર કરી દીધા હોય, તો તમારી વપરાશકર્તા ઍક્સેસને તરત જ લૉક કરો.
6. જો તમને તમારી અંગત માહિતી પ્રદાન કરવા માટે અથવા બેંકની સાઇટ પર તમારા એકાઉન્ટની વિગતો અપડેટ કરવા બદલ ઈ–મેલ/એસએમએસ/ફોન કૉલ પ્રાપ્ત થાય છે, તો લાલચમાં ન રહો.
7. તમે લૉગ ઇન થઈ ગયા પછી, તમને તમારું વપરાશકર્તા નામ અને લૉગિન પાસવર્ડ ફરીથી આપવા માટે કહેવામાં આવશે નહીં. ઉપરાંત, ઇન્ટરનેટ બેંકિંગનો ઉપયોગ કરતી વખતે તમને તમારા ક્રેડિટ અથવા ડેબિટ કાર્ડની વિગતો આપવા માટે કહેવામાં આવશે નહીં. જો તમને આવી માહિતી માટે પૂછતો સંદેશ (જેમ કે પોપ–અપ દ્વારા) મળે, તો આ માહિતી પ્રદાન કરશો નહીં, પછી ભલે તે પૃષ્ઠ ભલે 'અસલ' પૃષ્ઠ જેવું જ હોય. આવા પોપ–અપ્સ મોટાભાગે તમારા કોમ્પ્યૂટરને સંક્રમિત કરતા માલવેરનું પરિણામ હોય શકે છે.

★ **નીચેના મુદ્દાઓનું પાલન કરવાથી તમારી ઇન્ટરનેટ બેંકિંગની સુરક્ષામાં સુધારો થશેઃ**

1. નવીનતમ સુરક્ષા પેચ સાથે ઓપરેટિંગ સિસ્ટમનું નવું સંસ્કરણ (Version).
2. બ્રાઉઝર્સનું નવીનતમ સંસ્કરણ (Version).
3. ફાયરવોલને હંમેશાં ચાલુ સ્થિતિમાં રાખવી.

4. એન્ટિવાયરસ તેના લેટેસ્ટ વર્ઝન પ્રમાણે અપડેટેડ રાખવું.
5. સિસ્ટમ વાયરસ/ટ્રોજન મુકત છે તેની ખાતરી કરવા માટે તમારા કોમ્પ્યૂટરને નિયમિતપણે એન્ટિવાયરસથી સ્કેન કરો.
6. સમયાંતરે તમારો ઈન્ટરનેટ બેંકિંગ પાસવર્ડ બદલો.
7. પોસ્ટ લોગિન પેજમાં હંમેશાં છેલ્લી લોગ–ઈન તારીખ અને સમય તપાસો.
8. સાયબર કાફે અથવા શેર કરેલ કોમ્પ્યૂટર સિસ્ટમમાંથી ઈન્ટરનેટ બેંકિંગ એકાઉન્ટ્સ એક્સેસ કરવાનું ટાળો.

• સારાંશ

ઈન્ટરનેટ બેન્કિંગે આપણા જીવનને કેટલું સરળ બનાવી દીધું છે તેમાં કોઈ શંકા નથી. આજે આપણે કોઈપણ સમયે, ગમે ત્યાંથી પોતાના ખાતાની માહિતી મેળવી શકીએ છીએ, પૈસા ટ્રાન્સફર કરી શકીએ છીએ અને અન્ય ઘણી બધી બેંકિંગ સેવાઓનો લાભ લઈ શકીએ છીએ. ટેક્નોલોજીના આ યુગમાં ઈન્ટરનેટ બેન્કિંગ એક અનિવાર્ય ભાગ બની ગયું છે.

જોકે, આ સુવિધાઓ સાથે સાથે કેટલીક ચિંતાઓ પણ સામે આવી છે. સાયબર અપરાધના વધતા જતા કિસ્સાઓમાં ઈન્ટરનેટ બેન્કિંગ પણ એક લક્ષ્ય બની ગયું છે. ફિશિંગ, ફ્રોડ અને અન્ય ઘણી બધી સાયબર હુમલાઓ દ્વારા લોકોના ખાતાઓમાંથી પૈસા ચોરાઈ જાય છે. આવી સ્થિતિમાં, ઈન્ટરનેટ બેન્કિંગનો ઉપયોગ કરતી વખતે સુરક્ષાના પગલાં લેવાનું ખૂબ જ જરૂરી છે.

નિષ્કર્ષમાં કહી શકાય કે, ઈન્ટરનેટ બેન્કિંગ એ એક અદ્ભુત શોધ છે જેણે આપણા જીવનને સરળ બનાવ્યું છે. પરંતુ, આ સુવિધાનો લાભ લેતી વખતે સુરક્ષા અંગે સતર્ક રહેવું પણ જરૂરી છે. મજબૂત પાસવર્ડ બનાવવા, ફિશિંગ મેસેજ પર ક્લિક ન કરવું, અને બેંક દ્વારા આપવામાં આવેલી સુરક્ષા સુવિધાઓનો ઉપયો કરવો એ કેટલીક મહત્ત્વની બાબતો છે.

આ સાથે, બેંકોએ પણ ગ્રાહકોને સાયબર અપરાધોથી બચાવવા માટે સતત પ્રયત્નો કરવા જોઈએ. નવી-નવી ટેક્નોલોજીનો ઉપયોગ કરીને, બેંકોએ ગ્રાહકોના ખાતાઓને વધુ સુરક્ષિત બનાવવા માટે કામ કરવું જોઈએ.

આમ, ઈન્ટરનેટ બેન્કિંગ એ એક શક્તિશાળી સાધન છે જેનો ઉપયોગ જો સમજપૂર્વક કરવામાં આવે તે આપણા માટે ખૂબ જ ઉપયોગી સાબિત થઈ શકે છે.

3.8 તમારી પ્રગતિ ચકાસો

1. ઈન્ટરનેટ બેંકિંગની વ્યાખ્યા જણાવો.

____

____

____

2. ઈન્ટરનેટ બેંકિંગના પ્રકારો વિશે સમજાવો.

____

____

____

3. ઈન્ટરનેટ બેંકિંગની કાર્યપ્રણાલી વિશે સમજાવો

4. ઈન્ટરનેટ બેંકિંગના ફાયદા તથા ગેરફાયદા વિશે ચર્ચા કરો

5. સુરક્ષિત ઈન્ટરનેટ બેંકિંગ માટે યોગ્ય સૂચના વિશે માહિતી આપો.

3.9 ચાવીરૂપ શબ્દો

1. **વેબ સર્વર :** કમ્પ્યૂટર સિસ્ટમ જેના થકી ઈન્ટરનેટ બેન્કિંગ સેવાઓ શક્ય બને છે.
2. **નેટબેંકિંગ :** ઈન્ટરનેટ થકી કરાતું બેન્કિંગનું કામ

3.8 સંદર્ભસૂચિ

1. Dr. C. Nithya, (2021),"A STUDY OF ELECTRONIC BANKING IN INDIA", International Journal of Advanced Research in Commerce, Management & Social Science, ISSN : 2581-7930, Vol 04, 2021
2. Internet Banking by Dr. Ashok Kumar Singh, Calvin Publication, 2019
3. E-Banking in India: Challenges and Opportunities by Rimpi Jatana and R. K. Uppal, New Century Publications, 2007
4. www.rbi.org.in

એકમ-4 નેટવર્ક સુરક્ષા (Network Security)

: રૂપરેખા :

4.0 ઉદ્દેશો

4.1 પ્રસ્તાવના

4.2 ખ્યાલ

4.3 સુરક્ષા વ્યવસ્થાપન

4.4 ઈ-મેલ સુરક્ષા

4.5 વેબ સુરક્ષા

4.6 વાઈ-ફાઈ સુરક્ષા

● સારાંશ

4.7 તમારી પ્રગતિ ચકાસો

4.8 ચાવીરૂપ શબ્દો

4.9 સંદર્ભસૂચિ

4.0 ઉદ્દેશો

વિદ્યાર્થીમિત્રો, આ પ્રકરણનાં અભ્યાસ બાદ તમે,

– નેટવર્ક સુરક્ષાનો ખ્યાલ સમજી શકશો.

– સુરક્ષા વ્યવસ્થાની માહિતી મેળવશો.

– ઇ-મેઈલ સુરક્ષા વિશે જાણી શકશો.

– વેબ-સુરક્ષાને સમજી શકશો.

– વાઈ-ફાઈ સુરક્ષાની ચર્ચા કરી શકશો.

4.1 પ્રસ્તાવના

આ પ્રકરણ નેટવર્ક અને ઇન્ટરનેટ સુરક્ષા પરનું છે. સુરક્ષા સંબંધિત વિવિધ ખ્યાલ અને તકનીકી સમજતા પહેલા, તે જાણવું જરૂરી છે કે આપણે શું સુરક્ષિત કરવાનો પ્રયાસ કરી રહ્યા છીએ. જ્યારે આપણે કમ્પ્યૂટર, કમ્પ્યૂટર નેટવર્ક અને તે બધામાં સૌથી મોટા નેટવર્ક, ઇન્ટરનેટનો ઉપયોગ કરીએ ત્યારે વિવિધ જોખમો શું છે ? સંભવિત મુશ્કેલીઓ શું છે ? જો આપણે યોગ્ય સુરક્ષા નીતિઓ, ફ્રેમવર્ક અને ટૅક્નોલૉજીના અમલીકરણને સેટઅપ નહીં કરીએ તો શું થઈ શકે ? આ પ્રકરણ આ મૂળભૂત પ્રશ્નોના જવાબો આપવાનો પ્રયાસ કરવામાં આવ્યો છે.

શા માટે સુરક્ષા પ્રથમ સ્થાને જરૂરી છે? યોગ્ય સુરક્ષા ઈન્ફ્રાસ્ટ્રક્ચર પ્રદાન કરે છે. ખાસ કરીને આ દિવસોમાં જ્યારે ઇન્ટરનેટ પર આટલી મોટી હદે ગંભીર વ્યાપાર અને અન્ય પ્રકારના વ્યવહારો હાથ ધરવામાં આવે છે, ત્યારે અપૂરતી અથવા અયોગ્ય સુરક્ષા વ્યવસ્થાઓ સમગ્ર વ્યવસાયને નીચે લાવી શકે છે, અથવા લોકોના જીવન સાથે પાયમાલ કરી શકે છે!!!

સુરક્ષાના મુખ્ય સિદ્ધાંતો અમને વિવિધ ક્ષેત્રોને ઓળખવામાં મદદ કરે છે, જે સુરક્ષા જોખમો અને તેનો સામનો કરવા માટેના સંભવિત ઉકેલો નક્કી કરતી વખતે નિર્ણાયક છે.

4.2 ખ્યાલ

નેટવર્ક સુરક્ષા શું છે ?

SANS (SysAdmin, Audit, Network and Security - SANS ઈન્સ્ટિટ્યૂટ એ 1989 માં સ્થપાયેલી ખાનગી યુએસ ફોર-પ્રોફિટ કંપની છે જે માહિતી સુરક્ષા, સાયબર સુરક્ષા તાલીમ અને પ્રમાણપત્રો વેચવામાં નિષ્ણાત છે) સંસ્થાના જણાવ્યા મુજબ, નેટવર્ક સુરક્ષા એ અંતર્ગત નેટવર્કિંગ ઈન્ફ્રાસ્ટ્રક્ચરને અનધિકૃત ઍક્સેસ, દુરુપયોગ, ખામી, ફેરફાર, વિનાશ અથવા અયોગ્ય જાહેરાતથી બચાવવા માટે નિવારક પગલાં લેવાની પ્રક્રિયા છે. આ પગલાંને અમલમાં મૂકવાથી કમ્પ્યૂટર્સ, વપરાશકર્તાઓ અને પ્રોગ્રામ્સ સુરક્ષિત વાતાવરણમાં તેમના અનુમતિ પ્રાપ્ત મહત્ત્વપૂર્ણ કાર્યો કરવા માટે પરવાનગી આપે છે.

નેટવર્કને સુરક્ષિત કરવા માટે હાર્ડવેર ઉપકરણો, જેમ કે રાઉટર્સ, ફાયરવોલ અને એન્ટિ-માલવેર સોફ્ટવેર એપ્લિકેશન્સના જટિલ સંયોજનની જરૂર છે. સરકારી એજન્સીઓ અને વ્યવસાયો સુરક્ષા યોજનાઓ અમલમાં મૂકવા અને આ યોજનાઓની અસરકારકતા પર સતત દેખરેખ રાખવા માટે અત્યંત કુશળ માહિતી સુરક્ષા વિશ્લેષકોને નિયુક્ત કરે છે. દરેક સંસ્થા, કદ, ઉદ્યોગ અથવા ઇન્ફ્રાસ્ટ્રક્ચરને ધ્યાનમાં લીધા વિના, તેને આજે સાયબર ધમકીઓના સતત વધી રહેલા લેન્ડસ્કેપથી બચાવવા માટે નેટવર્ક સુરક્ષા ઉકેલોની જરૂર છે.

આજનું નેટવર્ક આર્કિટેકચર જટિલ છે અને તે એવા જોખમી વાતાવરણનો સામનો કરે છે જે હંમેશાં બદલાતા રહે છે. હુમલાખોરો હંમેશાં નબળાઈઓને શોધવા અને તેનું શોષણ કરવાનો સતત પ્રયાસ કરતા જ હોય છે. આ નબળાઈઓ ઉપકરણો, ડેટા, એપ્લિકેશન્સ, વપરાશકર્તાઓ અને સ્થાનો સહિત વિશાળ સંખ્યામાં અનેક વિસ્તારોમાં હોઈ શકે છે. આ કારણોસર જ, આજે ઘણા નેટવર્ક સુરક્ષા વ્યવસ્થાપન સાધનો અને એપ્લિકેશનો બધી જ જગ્યાએ ઉપયોગમાં પણ હોઈ છે જે વ્યક્તિગત ધમકીઓ અને શોષણને સંબોધિત કરે છે અને નિયમનકારી બિન-અનુપાલન પણ કરે છે. જ્યારે ડાઉનટાઈમની માત્ર થોડી મિનિટો વ્યાપક વિક્ષેપ અને સંસ્થાની બોટમ લાઇન અને પ્રતિષ્ઠાને મોટા પ્રમાણમાં નુકસાન પહોંચાડી શકે છે, ત્યારે આ રક્ષણાત્મક પગલાં અમલમાં હોવા જરૂરી છે.

- **નેટવર્ક સુરક્ષા શા માટે મહત્ત્વપૂર્ણ છે ?**

2020 એ વિશ્વભરમાં અસાધારણ વલણો અને અણધારી ઘટનાઓથી ભરેલું વર્ષ હતું. રોગચાળાએ શાબ્દિક રીતે વ્યવસાયો ચલાવવાની રીત બદલી નાખી છે. ઘણા કર્મચારીઓ કે જેમણે એક સમયે ક્યુબિકલ અથવા ઓપન-સ્પેસ ડેસ્ક પર કબજો કર્યો હતો તેઓ હવે અનિશ્ચિત સમયગાળા માટે દૂરસ્થ રીતે કામ કરી રહ્યા છે. રસપ્રદ વાત એ છે કે, જે વ્યવસાયો પાસે રિમોટ વર્કફોર્સને ટેકો આપવા માટે ટેક્નોલૉજી પ્રદાન કરવાના માધ્યમો છે તેઓ ખૂબ સારી રીતે અનુકૂલિત થયા છે, અને ઘણા ઈ-કોમર્સ વ્યવસાયો નફાકારક બનવાનું ચાલુ રાખે છે. જો કે ઘણી સંસ્થાઓએ પડકારનો સામનો કર્યો છે અને દૂરસ્થ કાર્યબળને સ્વીકાર્યું છે, આ વલણે સાયબર હુમલાની હાજરીને અટકાવી નથી. હકીકતમાં, તે ફક્ત જોખમી હુમલાખોરો માટે બીજી તક પૂરી પાડી છે. ફેબ્રુઆરી 2020થી રેન્સમવેર હુમલા બેઝલાઇન સ્તરો કરતાં 148% વધ્યા છે. આ વધારો મુખ્યત્વે ઘર-આધારિત વપરાશકર્તાઓ સામે સીધા હુમલાનું પરિણામ છે. સર્વર, ડેટાબેસેસ, વેબ એપ્લિકેશન અને કલાઉડ એપ્લિકેશન્સો ખસેડાયા નથી, જો કે, તેમને ઍક્સેસ કરનારા કર્મચારીઓ હવે દૂરસ્થ છે. સંસ્થાઓ કર્મચારીઓને સુરક્ષા-જાગૃત રહેવાની તાલીમ આપવા માટે સક્ષમ હોવા જોઈએ.

નેટવર્ક સિક્યોરિટી હોમ નેટવર્ક તેમજ બિઝનેસ જગતમાં મહત્ત્વપૂર્ણ છે. હાઇ-સ્પીડ ઇન્ટરનેટ કનેકશન ધરાવતા મોટાભાગના ઘરોમાં એક અથવા વધુ વાયરલેસ રાઉટર હોય છે, જે યોગ્ય રીતે સુરક્ષિત ન હોય તો તેનો ઉપયોગ કોઈ પણ બહારનો વ્યક્તિ કરી શકે છે.

એક નક્કર નેટવર્ક સુરક્ષા સિસ્ટમ ડેટા નુકસાન, ચોરી અને તોડફોડના જોખમને ઘટાડવામાં મદદ કરે છે. હેકર્સ, અસંતુષ્ટ કર્મચારીઓ અથવા સંસ્થામાં નબળી સુરક્ષા પદ્ધતિઓ વેપાર રહસ્યો અને ગ્રાહકોની ખાનગી વિગતો સહિત ખાનગી ડેટાને ખુલ્લા મૂકી શકે છે.

ગોપનીય સંશોધન ગુમાવવાથી, ઉદાહરણ તરીકે, સંસ્થાને તે મેળવવા માટે ચૂકવેલ સ્પર્ધાત્મક લાભો છીનવીને લાખો રૂપિયાનું સંભવતઃ ખર્ચ થઈ શકે છે. જ્યારે હેકર્સ ગ્રાહકોની વિગતોની ચોરી કરે છે અને છેતરપિંડી માટે તેનો ઉપયોગ કરે છે, ત્યારે સંસ્થા પ્રત્યે નકારાત્મક પ્રચાર અને જાહેરમાં અવિશ્વાસ પેદા કરે છે.

નેટવકર્સ સામેના મોટાભાગના સામાન્ય હુમલાઓ નેટવર્કને નુકસાન પહોંચાડવાને બદલે વપરાશકર્તાઓના સંદેશાવ્યવહાર અને ડેટા પર જાસૂસી કરીને માહિતીની ઍક્સેસ મેળવવા માટે રચાયેલ છે. તેઓ વપરાશકર્તાઓના ઉપકરણોને નુકસાન પહોંચાડી શકે છે અથવા સુવિધાઓની ભૌતિક ઍક્સેસ મેળવવા માટે સિસ્ટમમાં ચાલાકી કરી શકે છે. આ સંસ્થાની મિલકત અને સભ્યોને નુકસાનના જોખમમાં મૂકે છે.

સક્ષમ નેટવર્ક સુરક્ષા પ્રક્રિયાઓ ડેટાને સુરક્ષિત રાખે છે અને નબળી સિસ્ટમ્સને બહારના હસ્તક્ષેપથી અવરોધે છે. આ નેટવર્કના વપરાશકર્તાઓને સુરક્ષિત રહેવા અને સંસ્થાના લક્ષ્યોને પ્રાપ્ત કરવા પર ધ્યાન કેન્દ્રિત કરવાની મંજૂરી આપે છે. તેનાથી વધુ, તેનો અર્થ એ છે કે ગ્રાહકો અને ભાગીદારો પણ સંસ્થા સાથે વિશ્વાસપૂર્વક સંપર્ક કરી શકે છે. સિસ્કો કહે છે તેમ 'નેટવર્ક સુરક્ષા સંસ્થાની પ્રતિષ્ઠાને સુરક્ષિત કરે છે.'

★ **માહિતી સુરક્ષા (Information Security)ની જરૂરિયાત નીચેના મુદ્દાઓ પર આધારિત છે :**

- કોઈપણ અનિચ્છનીય ઍક્સેસ સામે માહિતીનું રક્ષણ કરવા માટે.
- રૂટમાં કોઈપણ અયોગ્ય વિલંબ (delay) થી ડેટાને સુરક્ષિત રાખવા માટે તેને ઇચ્છિત સમયગાળામાં ગંતવ્ય સ્થાન (destination) પર પહોંચાડવા માટે.
- કોઈપણ અનિચ્છનીય સુધારાથી ડેટાને બચાવવા માટે.
- નેટવર્કમાં કોઈ ચોક્કસ વપરાશકર્તાને કોઈપણ મેલ મોકલવાથી પ્રતિબંધિત કરવા માટે, સંદેશ એવી રીતે મોકલો કે જેમાં તે પ્રાપ્ત કરનાર પક્ષને લાગે કે તે કોઈ તૃતીય પક્ષ દ્વારા મોકલવામાં આવ્યો છે. (સંસાધન સંદેશના મૂળ પ્રેષકની ઓળખ છુપાવવાથી રક્ષણ).
- હાર્ડવેર જેવા કે હાર્ડ ડિસ્ક, પીસી, લેપટોપને માલવેર, વાયરસ વગેરેના હુમલાથી બચાવવા માટે, જે સિસ્ટમમાં સંગ્રહિત તમામ દૂષિત સામગ્રીને કાઢી નાખીને નુકસાનથી બચાવવા માટે.
- સિસ્ટમને ટ્રોજન હોર્સ, વોર્મ્સ વગેરેથી સુરક્ષિત રાખવા માટે જે આપણી સિસ્ટમને સંપૂર્ણપણે નષ્ટ કરી શકે છે.

4.3 સુરક્ષા વ્યવસ્થાપન

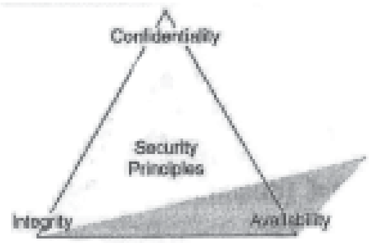
★ સુરક્ષા સિદ્ધાંત (Security Principles)

સુરક્ષા કાર્યક્રમનું સંચાલન કેવી રીતે કરવું તે સમજવા માટે, મૂળભૂત સિદ્ધાંતો સમજવા

આવશ્યક છે. માહિતીને શા માટે રક્ષણની જરૂર છે તે નિર્ધારિત કરવા માટે આ સિદ્ધાંતો બિલ્ડીંગ બ્લોક્સ છે.

માહિતી સુરક્ષા (ઇન્ફોસેક) સમુદાયમાં, '**CIA**' ને ગોપનીયતા (Confidentiality), અખંડિતતા (Intergrity) અને ઉપલબ્ધતા (Availability) માટે વપરાય છે, અન્યથા CIA triad તરીકે ઓળખાય છે.

એકસાથે, આ ત્રણ સિદ્ધાંતો કોઈપણ સંસ્થાના સુરક્ષા ઈન્ફ્રાસ્ટ્રક્ચરનો આધાર બનાવે છે; વાસ્તવમાં, તેઓ દરેક સુરક્ષા કાર્યક્રમ માટે લક્ષ્યો અને ઉદ્દેશ્યો તરીકે કાર્ય કરે છે CIA ટ્રાયડ માહિતી સુરક્ષા માટે એટલી પાયાની છે કે ગમે ત્યારે ડેટા લીક થાય છે, સિસ્ટમ પર હુમલો થાય છે, વપરાશકર્તા ફિશિંગ ગ્રહણ કરે છે, એકાઉન્ટ હાઈજેક થાય છે, વેબસાઇટ દૂષિત રીતે ડાઉન કરવામાં આવે છે, અથવા અન્ય કોઈપણ સુરક્ષા ઘટનાઓ થાય છે ત્યારે જાણી શકાય છે કે આમાંના એક અથવા વધુ સિદ્ધાંતોનું ઉલ્લંઘન કરવામાં આવ્યું છે કે કેમ. **(જુઓ આકૃતિ 4.1)**.



આકૃતિ 4.1 : સુરક્ષાના મૂળભૂત સિદ્ધાંતો ગોપનીયતા, અખંડિતતા અને ઉપલબ્ધતા

1. ગોપનીયતા (Confidentiality)

ગોપનીયતા માહિતીની ગુપ્તતા નક્કી કરે છે. ગોપનીયતાને ધ્યાનમાં લેતી વખતે, મેનેજર ડેટાને કેવી રીતે અને કયાં એકસેસ કરી શકાય તેના સંદર્ભમાં ઍકસેસનું સ્તર નક્કી કરે છે. માહિતી સંસ્થાને ઉપયોગી થાય તે માટે, તેને ગોપનીયતાની ડિગ્રી દ્વારા વર્ગીકૃત કરી શકાય છે.

હુમલાખોરોને નિર્ણાયક ડેટાની ઍકસેસ મેળવવાથી રોકવા માટે, જે વપરાશકર્તાને ગોપનીય ડેટાની ઍકસેસની મંજૂરી આપવામાં આવી શકે છે તેને બાહ્ય એકસેસ પોર્ટથી સેવાને ઍકસેસ કરવાની મંજૂરી આપવામાં આવશે નહીં. ગોપનીયતાનું સ્તર ઉપલબ્ધતાનું સ્તર નક્કી કરે છે જે વિવિધ એકસેસ કંટ્રોલ મિકેનિઝમ્સ દ્વારા નિયંત્રિત થાય છે. સામાન્ય રીતે, આમાં એ સુનિશ્ચિત કરવાનો સમાવેશ થાય છે કે જેઓ અધિકૃત છે તેમની પાસે જ ચોક્કસ સંપત્તિની ઍકસેસ છે અને જેઓ અનધિકૃત છે તેમને ઍકસેસ મેળવવાથી સક્રિયપણે અટકાવવામાં આવે છે.

ગોપનીય ડેટાને આપવામાં આવતી સુરક્ષા—સુરક્ષા પ્રોગ્રામ જેટલી જ સારી છે. ગોપનીયતા જાળવવા માટે, સુરક્ષા પ્રોગ્રામે ડેટા વાંચવા માટે નેટવર્કનું નિરીક્ષણ કરતા હુમલાખોરના પરિણામોને ધ્યાનમાં લેવું આવશ્યક છે. જો કે એવા ઘણા બધા ટૂલ્સ ઉપલબ્ધ છે જે હુમલાખોરને આ રીતે ડેટા વાંચતા અટકાવી શકે છે, આ ઉપરાંત ટ્રાન્સમિશનના બિંદુઓ પર સલામતીનાં પગલાં હોવા જોઈએ, જેમ કે એનક્રિપ્શનનો ઉપયોગ કરીને અથવા નેટવર્કને ભૌતિક રીતે સુરક્ષિત કરીને.

ગોપનીયતા માટેનો બીજો હુમલો ડેટાને ઍકસેસ કરવા અથવા ઍકસેસ મેળવવા માટે સોશિયલ એન્જિનિયરિંગનો ઉપયોગ છે. સોશિયલ એન્જિનિયરિંગનો બચાવ કરવો

મુશ્કેલ છે કારણ કે તેને વ્યાપક અને સક્રિય સુરક્ષા જાગૃતિ કાર્યક્રમની જરૂર છે.

2. અખંડિતતા (Integrity)

અખંડિતતા ખાતરી આપે છે કે ડેટા સચોટ અને વિશ્વસનીય છે. અખંડિતતા વિના, ડેટા એકત્રિત કરવા અને જાળવવાની કિંમતને ન્યાયી ઠેરવી શકાતી નથી. તેથી, નીતિઓ અને પ્રક્રિયાઓએ ખાતરી કરવી જોઈએ કે ડેટા પર વિશ્વાસ કરી શકાય કે કેમ.

માહિતીની અખંડિતતાને સુનિશ્ચિત કરવા માટે મૂકવામાં આવેલી પદ્ધતિઓએ તે ડેટાના સંગ્રહ (દૂષણ) અને તેના પ્રસારણ (દખલ) પરના હુમલાઓને અટકાવવા જોઈએ. સ્ટોરેજ અને યુઝરના વર્કસ્ટેશન વચ્ચે નેટવર્ક પર બદલાયેલો ડેટા એટલો જ અવિશ્વસનીય હોઈ શકે છે જેટલો હુમલાખોર સ્ટોરેજ મીડિયા પરના ડેટાને બદલી અથવા કાઢી નાખે છે. ડેટાને સુરક્ષિત કરવામાં સ્ટોરેજ અને નેટવર્ક મિકેનિઝમ બંનેનો સમાવેશ થાય છે.

હુમલાખોરો ડેટાને દૂષિત કરવા માટે ઘણી પદ્ધતિઓનો ઉપયોગ કરી શકે છે. વાયરસ મીડિયામાં સૌથી વધુ વારંવાર નોંધાય છે. હુમલો શરૂ થયા પછી, તેને રોકવું મુશ્કેલ બની શકે છે અને આ રીતે ડેટાની અખંડિતતાને અસર થાય છે. આ હુમલાઓને રોકવા માટે ઉપયોગમાં લઈ શકાય તેવા કેટલાક રક્ષણોમાં ઘૂસણખોરી શોધ, એન્ક્રિપ્શન અને કડક ઍક્સેસ જ નિયંત્રણો છે.

બધા અખંડિતતા હુમલાઓ દૂષિત નથી. વપરાશકર્તાઓ અજાણતામાં ખોટી ડેટા એન્ટ્રી, પ્રોગ્રામ ચલાવવામાં લેવામાં આવેલ ખોટો નિર્ણય અથવા પ્રક્રિયાઓનું પાલન ન કરીને અચોક્કસ અથવા અમાન્ય ડેટા સ્ટોર કરી શકે છે. તેઓ તેમના વર્કસ્ટેશન પર સિસ્ટમ રૂપરેખાંકન ભૂલો દ્વારા અથવા ડેટાને ઍક્સેસ કરવા માટે ખોટા પ્રોગ્રામનો ઉપયોગ કરીને પણ અખંડિતતાને અસર કરી શકે છે. આને રોકવા માટે, વપરાશકર્તાઓને તેમની માહિતી સુરક્ષા જાગૃત્તતા તાલીમ દરમિયાન ડેટા અખંડિતતા વિશે શીખવવું જોઈએ. વધુમાં, પ્રોગ્રામ્સને સિસ્ટમમાં સંગ્રહિત કરતા પહેલા ડેટાની અખંડિતતા ચકાસવા માટે ગોઠવેલ હોવા જોઈએ. નેટવર્ક વાતાવરણમાં, ડેટાને તેના ફેરફારને રોકવા માટે એનક્રિપ્ટ કરી શકાય છે.

3. ઉપલબ્ધતા (Availability)

ઉપલબ્ધતા એ માહિતી સંપત્તિને ઍક્સેસ કરવાની વપરાશકર્તાઓની ક્ષમતા છે. માહિતીનો કોઈ ઉપયોગ નથી જો તે ઍક્સેસ કરી શકાતી નથી. વપરાશકર્તાની વિનંતીઓને સંતોષવા માટે સિસ્ટમો પાસે વપરાશ માટેની પૂરતી ક્ષમતા હોવી જોઈએ, અને નેટવર્ક આર્કિટેક્ટ્સ ઉપલબ્ધતાના ભાગ રૂપે ક્ષમતાને ધ્યાનમાં લેવી જોઈએ. ડિનાયલ–ઓફ–સર્વિસ (DOS) હુમલાઓને રોકવા માટે પ્રક્રિયાઓ બનાવવામાં આવે તે સ્પષ્ટ કરીને તેને લાગુ કરવા માટે નીતિઓ લખી શકાય છે.

માત્ર હુમલાખોરો સિસ્ટમ અને નેટવર્કની ઉપલબ્ધતાને અસર કરી શકે છે. પર્યાવરણ, હવામાન, અગ્નિ, વિદ્યુત સમસ્યાઓ અને અન્ય પરિબળો સિસ્ટમ અને નેટવર્કને કામ કરતા અટકાવી શકે છે. આ સમસ્યાઓને રોકવા માટે, તમારી સંસ્થાની ભૌતિક સુરક્ષા નીતિઓમાં ઉપલબ્ધતા જાળવવામાં મદદ કરવા માટે વિવિધ નિયંત્રણો અને પ્રક્રિયાઓનો ઉલ્લેખ કરવો જોઈએ.

તેમ છતાં ઍક્સેસનો અર્થ એ નથી કે ડેટા તરત જ ઉપલબ્ધ હોવો જોઈએ. માહિતીની ઉપલબ્ધતા એ ઓળખી લેવું જોઈએ કે વિનંતી પર તમામ ડેટા ઉપલબ્ધ હોવો જરૂરી નથી. કેટલાક ડેટાને મીડિયા પર સંગ્રહિત કરી શકાય છે જેને ઍક્સેસ કરવા માટે વપરાશકર્તા અથવા ઑપરેટરના હસ્તક્ષેપની જરૂર પડી શકે છે. ઉદાહરણ તરીકે, જો કોઈ સંસ્થા દરરોજ ગીગાબાઇટ્સ ડેટા એકત્રિત કરે છે, તો તેઓ પાસે તે બધો ઓનલાઈન સંગ્રહ કરવા માટે

સંસાધનો ન પણ હોય. આ ડેટાને ઑફલાઇન સ્ટોરેજ યુનિટ પર સ્ટોર કરી શકાય છે, જેમ કે સીડી જયુકબોકસ, જે તાત્કાલિક એકસેસ ઓફર કરતું નથી.

નેટવર્ક હુમલાના પ્રકારને આધારે અમે અમારી નેટવર્કિંગ સિસ્ટમને વિવિધ રીતે સુરક્ષિત કરી શકીએ છીએ.

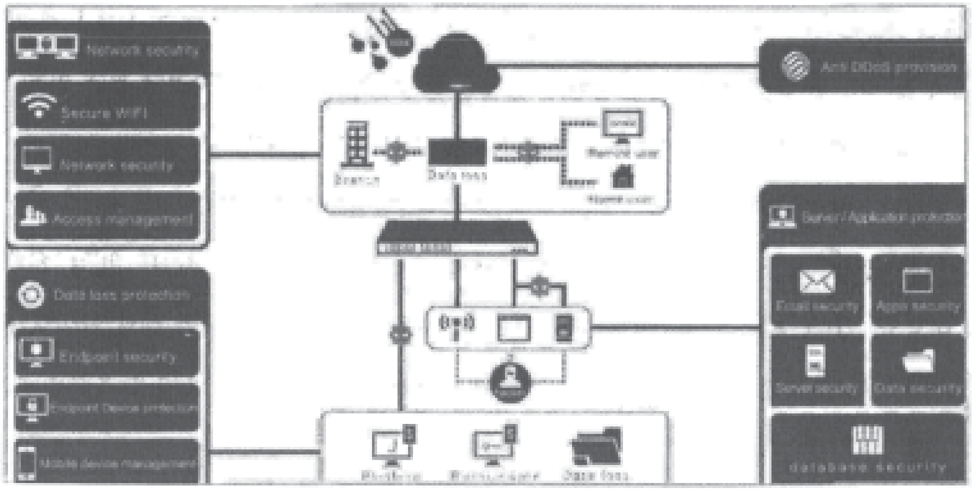
1. એન્ટિવાયરસ અને એન્ટિ–માલવેર સોફ્ટવેર :

એન્ટિવાયરસ સોફ્ટવેર એ એક પ્રકારનું સોફ્ટવેર છે જેનો ઉપયોગ કોમ્પ્યૂટરમાંથી વાયરસને રોકવા, સ્કેન કરવા, શોધવા અને કાઢી નાખવા માટે થાય છે. એકવાર ઈન્સ્ટોલ થઈ ગયા પછી, મોટાભાગના એન્ટિવાયરસ સોફ્ટવેર વાયરસ હુમલા સામે રિઅલ–ટાઈમ સુરક્ષા પ્રદાન કરવા માટે પૃષ્ઠભૂમિમાં આપમેળે ચાલશે. દરરોજ અસંખ્ય નવા વાઈરસ શોધવામાં આવે છે, તેથી ઈન્ટરનેટ પર પ્રચલિત દૂષિત કોડના ટનથી આગળ રહેવા માટે નવીનતમ શોધ ફાઈલોમાં આપમેળે અપડેટ થવા માટે એન્ટીવાયરસ સૉફ્ટવેર ઈન્સ્ટોલ અને ગોઠવેલું હોવું મહત્ત્વપૂર્ણ છે. મૉલવેર સર્જકો આજે કમ્પ્યૂટર સિસ્ટમમાં નબળાઈઓનો કેવી રીતે ઉપયોગ કરવો તે અંગે ખરેખર જાણકાર છે.

કોમ્પ્યૂટર સિસ્ટમને વાયરસથી સંક્રમિત થતા અટકાવવા માટે એન્ટિ-વાયરસ સોફ્ટવેરને સંરક્ષણના પ્રથમ સ્તર તરીકે તૈનાત કરી શકાય છે. આ સોફ્ટવેરનો ઉપયોગ માલવેર સામે રક્ષણ કરવા માટે થાય છે, જેમાં વાયરસ, ટ્રોજન, રેન્સમવેર અથવા સ્પાયવેરની કોઈપણ વસ્તુનો સમાવેશ થાય છે. સ્પષ્ટ કારણો ઉપરાંત, માલવેર ખૂબ જ ખતરનાક બની શકે છે કારણ કે કેટલીકવાર, તે તમારા નેટવર્કમાં દિવસો અને અઠવાડિયા સુધી શાંત રહી શકે છે, પછી ત્યાં ઉભરી આવવા અને હુમલો કરવા માટે તૈયાર બેસી રહે છે. એન્ટિવાયરસ અને એન્ટિમૅલવેર સૉફ્ટવેર માલવેર એન્ટ્રી માટે સ્કેન કરીને અને ફાઈલોને ટ્રેક કરીને પછીથી આ ખતરાનો સામનો કરે છે.

2. ડેટા લોસ પ્રિવેન્શન (DLP):

MNC અથવા મોટા પાયાની સંસ્થાઓ, તેમની આંતરિક માહિતી કોઈપણ કર્મચારી દ્વારા બહારની દુનિયામાં લીક ન થાય તેની ખાતરી કરીને ડેટા અને સંસાધનોની ગુપ્તતા જાળવી રાખે છે. આ ગુપ્તતા DLP ટૅક્નોલૉજીનો ઉપયોગ કરીને કરવામાં આવે છે, જેમાં નેટવર્ક એડમિનિસ્ટ્રેટર માહિતીને ફોરવર્ડ કરવા, અપલોડ કરવા અથવા છાપવા માટે પોર્ટ્સ (Ports) અને સાઈટ્સને અવરોધિત કરીને તેને બહારની દુનિયામાં શેર કરવાથી અટકાવવા માટે કર્મચારીની માહિતીની ઍકસેસને પ્રતિબંધિત કરે છે.



આકૃતિ 4.2 : સિસ્ટમમાં વિવિધ સ્તરે સુરક્ષા જોગવાઈઓના પ્રકાર

3. ઈ-મેલ સુરક્ષા

ઈ-મેઈલ વ્યવસાય માટે ખૂબ જ મહત્ત્વપૂર્ણ છે, અને ઈ-મેઈલ ગેટવે એ સુરક્ષા ભંગ માટે મુખ્ય ખતરો છે તે ધ્યાનમાં લેતા, ઈ-મેઈલ સુરક્ષા એ એકદમ જરૂરી છે. હુમલાખોરો તમારી વ્યક્તિગત માહિતીનો ઉપયોગ તમામ પ્રકારના નુકસાન કરવા માટે કરી શકે છે, જેમ કે તમારા ક્લાયંટને છેતરવા અને તેમને માલવેરથી ભરેલી સાઇટ્સ પર મોકલવા માટે તમારા વતી બ્લેકમેલ અથવા ઈ-મેલ કરવા. ઇ-મેઇલ સુરક્ષા એપ્લિકેશન આ હુમલાઓને અવરોધિત કરવામાં અને શું મોકલવામાં આવે છે તેને નિયંત્રિત કરવામાં મદદ કરી શકે છે.

4. ફાયરવોલ્સ :

આ નેટવર્કિંગ સિસ્ટમનો અભિન્ન ભાગ છે જે બે નેટવર્ક વચ્ચે અથવા બે ઉપકરણો વચ્ચે દિવાલ તરીકે કામ કરે છે. તે મૂળભૂત રીતે પૂર્વ-નિર્ધારિત નિયમોનો સમૂહ છે જેનો ઉપયોગ નેટવર્કને કોઈપણ અનધિકૃત ઍક્સેસથી રોકવા માટે થાય છે. ફાયરવોલ બે પ્રકારના હોય છે, હાર્ડવેર અને સૉફ્ટવેર, સૉફ્ટવેર ફાયરવૉલ વિવિધ પ્રકારના હુમલાઓથી રક્ષણ પૂરું પાડવા માટે સિસ્ટમ્સમાં ઇન્સ્ટોલ કરેલું છે કારણ કે તે નેટવર્કમાં અનિચ્છનીય જીવોને ફિલ્ટર, અવરોધિત અને ઠીક કરે છે. જ્યારે હાર્ડવેર ફાયરવોલ બે નેટવર્કિંગ સિસ્ટમો વચ્ચેના ગેટવે તરીકે કામ કરે છે જેથી કરીને માત્ર ચોક્કસ પૂર્વ-વ્યાખ્યાયિત વપરાશકર્તા અથવા ટ્રાફિક નેટવર્ક અને તેના સંસાધનોને ઍક્સેસ કરી શકે.

5. ઘૂસણખોરી નિવારણ સિસ્ટમ (IPS):

તે નેટવર્ક સુરક્ષા સિસ્ટમ છે જેમાં કેટલાક નિયમોનો સમાવેશ થાય છે અને તેને અનુસરીને તમે જોખમોને સરળતાથી શોધી શકો છો અને તેને અવરોધિત પણ કરી શકો છો.

6. મોબાઈલ સુરક્ષા :

સાયબર-ગુનેગારો હેન્ડસેટ પરની ડેટા સુવિધા સાથે મોબાઇલ હેન્ડસેટને સરળતાથી હેક અથવા હુમલો કરી શકે છે, અને તેઓ વેબસાઇટની કોઈપણ અસુરક્ષિત સંસાધન લિંકથી ઉપકરણમાં પ્રવેશ કરી શકે છે. તેથી મોબાઇલ ઉપકરણ પર એન્ટિવાયરસ ઇન્સ્ટોલ કરવું જરૂરી છે અને લોકોએ વિશ્વસનીય સ્ત્રોતોમાંથી ડેટા ડાઉનલોડ અથવા અપલોડ કરવો જોઈએ અને તે પણ ફક્ત સુરક્ષિત વેબસાઇટ્સમાંથી જ.

7. નેટવર્ક વિભાજન :

સુરક્ષાના દૃષ્ટિકોણ માટે, સૉફ્ટવેર આધારિત સંસ્થા તેમના નિર્ણાયક ડેટાને બે અથવા ત્રણ ભાગોમાં વિભાજિત કરશે અને તેને વિવિધ સ્થળોએ અને કેટલાક સંસાધનો અથવા ઉપકરણો પર રાખશે. આવું એટલે કરવામાં આવે છે કે જેથી સૌથી ખરાબ કિસ્સામાં, જો કોઈ પણ સ્થાન પરનો ડેટા વાયરસના હુમલાથી દૂષિત અથવા કાઢી નાખવામાં આવ્યો હોય, તો તેને કોઈપણ બેકઅપ સ્ત્રોતોમાંથી ફરીથી ગોઠવી શકાય.

8) વેબ સુરક્ષાઃ

વેબ સિકયોરિટી એ વાઈરસ અને હેકર્સ માટે વધુ સંવેદનશીલ હોય તેવી સાઇટ્સને અવરોધિત કરીને વેબસાઇટ્સ અને URL ને મર્યાદિત ઍક્સેસની જોગવાઈનો સંદર્ભ આપે છે. આમ તે મૂળભૂત રીતે વેબ-આધારિત ધમકીઓને નિયંત્રિત કરવા સાથે સંબંધિત છે.

9. એન્ડપોઇન્ટ સુરક્ષા

નેટવર્ક સિકયોરિટીની સાથે નેટવર્ક એક્સેસ કંટ્રોલ, એપ્લીકેશન સિક્યુરિટી અને નેટવર્ક મોનિટરિંગ જેવા અન્ય નેટવર્ક સિક્યુરિટી ટૂલ્સને જોડીને એન્ડપોઇન્ટ સિકયોરિટી

પ્રાપ્ત થાય છે. એન્ડપોઈન્ટ ડિવાઈસ એ હાર્ડવેરનો કોઈપણ ભાગ છે જે લોકલ એરિયા નેટવર્ક (LAN) અથવા વાઈડ એરિયા નેટવર્ક (WAN) સાથે જોડાયેલ છે, જેમ કે વર્કસ્ટેશન, લેપટોપ, સ્માર્ટફોન, પ્રિન્ટર અને મોબાઈલ કિઓસ્ક. વિવિધ સોફ્ટવેર કે જેમાં ઈનબિલ્ટ-અદ્યતન એન્ડપોઈન્ટ સુરક્ષા સુવિધાઓ છે અને તેનો ઉપયોગ આ હેતુ માટે થાય છે. આ ફાઈલ પ્રતિષ્ઠા, ઓટો-સેન્ડબોક્સ, વેબફિલ્ટરિંગ, એન્ટિવાયરસ સોફ્ટવેર અને ફાયરવોલ સહિતની સુરક્ષાના સાત સ્તરો પ્રદાન કરે છે.

10. નેટવર્ક એકસેસ કંટ્રોલ (NAC)

તમારા નેટવર્કને કોણ ઍક્સેસ કરી શકે અને કોણ ન કરી શકે તે નિયંત્રિત કરો તેને NAC કહેવાય છે. તમારા નેટવર્કમાં કયા ઉપકરણો અને વપરાશકર્તાઓને મંજૂરી છે તે ઓળખીને તમે એકસેસ કંટ્રોલ કરો છો. અહીંથી તમે વિવિધ સુરક્ષા નીતિઓ લાગુ કરી શકો છો જેમ કે અમુક ઉપકરણોને અવરોધિત કરવા અને તમારા નેટવર્કમાં કોઈ શું કરી શકે તેનું નિયંત્રણ કરવું. સામાન્ય અને અસાધારણ વર્તન શું છે તે ઓળખવા માટે તમે વર્તણૂકીય વિશ્લેષણાત્મક સાધનોનો પણ ઉપયોગ કરી શકો છો. એકવાર તમે તે કરી લો, પછી તમે તેને સેટ કરી શકો છો જ્યાં જ્યારે પણ કંઈક અસામાન્ય રીતે કામ કરતું હોય ત્યારે તમને સૂચનાઓ મળશે.

11. વર્ચ્યુઅલ પ્રાઈવેટ નેટવર્ક (VPN):

રિમોટલી કનેકટેડ ડિવાઈસ અથવા નેટવર્ક પર ઈન્ટરનેટ પર પ્રમાણિકરણ અને ફ્લોટિંગ ડેટા ટ્રાફિક માટે એન્ક્રિપ્શન પદ્ધતિઓનો ઉપયોગ કરીને VPN નેટવર્કનો ઉપયોગ કરીને સિસ્ટમને અત્યંત સુરક્ષિત બનાવી શકાય છે. IPSec એ સૌથી વધુ ઉપયોગમાં લેવાતી પ્રમાણિકરણ પ્રક્રિયા છે.

12. એપ્લિકેશન સુરક્ષા

એપ્લિકેશન સિકયોરિટી એ અનધિકૃત ઍક્સેસ અને ફેરફાર જેવા જોખમો સામે સુરક્ષા નબળાઈઓને રોકવા માટે એપ્લિકેશનમાં સુરક્ષા સુવિધાઓ વિકસાવવા, ઉમેરવા અને પરીક્ષણ કરવાની પ્રક્રિયા છે. વેરાકોડના સ્ટેટ ઑફ સૉફ્ટવેર સિકયુરિટી રિપોર્ટ મુજબ, તેણે પરીક્ષણ કરેલ 85,000 એપ્લિકેશનોમાંથી 83%માં ઓછામાં ઓછી એક સુરક્ષા ખામી હતી. ઘણા પાસે ઘણું બધું હતું, કારણ કે તેમના સંશોધનમાં કુલ 10 મિલિયન ભૂલો જોવા મળી હતી, અને તમામ એપ્લિકેશન્સમાંથી 20%માં ઓછામાં ઓછી એક ઉચ્ચ ગંભીરતાની ખામી હતી. કોડમાં ખામીઓને ઓળખવા અને તેને ઘટાડવા માટે સંસ્થાઓ માટે નિયમિત એપ્લિકેશન સુરક્ષા પરીક્ષણ કરવું મહત્ત્વપૂર્ણ છે. આ સાયબર હુમલાખોરોને જટિલ વેબ અપ્લિકેશનો સાથે સમાધાન અથવા શોષણ કરતા અટકાવશે.

- **સિસ્ટમ અને નેટવર્કને સુરક્ષિત બનાવવાનાં પરિમાણો :**

સિસ્ટમને સુરક્ષિત બનાવવા માટેના મુખ્ય પરિમાણો નીચે મુજબ છે :

1. મજબૂત પાસવર્ડ્સ સેટ કરો :

સિસ્ટમ અથવા નેટવર્કને દૂષિત હુમલાઓથી બચાવવા માટે, સૌપ્રથમ લોગિન અને ઍક્સેસ માટે તમારી સિસ્ટમમાં મજબૂત પાસવર્ડ મૂકી શકાય અને પાસવર્ડમાં ઘણા બધા અક્ષર, પ્રતીક અને સંખ્યાઓ હોવા જરૂરી છે. જન્મદિવસનો પાસવર્ડ તરીકે ઉપયોગ કરવાનું ટાળવું જોઈએ કારણ કે તેને હેકર્સ સરળતાથી તોડી શકે છે.

2. ફાયરવોલ સ્થાપિત કરો :

નેટવર્કિંગ સિસ્ટમને અનિચ્છનીય ઍક્સેસ અથવા અન્ય જોખમોથી બચાવવા માટે હંમેશાં મજબૂત ફાયરવોલ મૂકો.

3. એન્ટિવાયરસ પ્રોટેકશનઃ

સિસ્ટમ અને લેપટોપને હંમેશાં એન્ટીવાયરસ સોફ્ટવેરથી ઇન્સ્ટોલ કરી શકાય. એન્ટિવાયરસ સોટવેર ચેપગ્રસ્ત ફાઈલોને સ્કેન કરશે, સ્પોટ કરશે અને ફિલ્ટર કરશે અને સિસ્ટમમાં વાયરસના હુમલાને કારણે ઊભી થતી સમસ્યાને પણ ઠીક કરશે.

4. વારંવાર અપડેટ કરોઃ

સિસ્ટમ અને નેટવર્કને એન્ટિવાયરસ સોફ્ટવેરના નવીનતમ સંસ્કરણ સાથે અપડેટ કરવા અને સિસ્ટમની જરૂરિયાત મુજબ સિસ્ટમ માટે નવીનતમ પેચો અને સ્ક્રિપ્ટ્સ ઇન્સ્ટોલ કરવા માટે ખૂબ જ મહત્ત્વપૂર્ણ છે. આનાથી વાયરસના હુમલાની શક્યતાઓ ઓછી થશે અને નેટવર્ક વધુ સુરક્ષિત બનશે.

5. લેપટોપ અને મોબાઈલ ફોનનું રક્ષણ કરોઃ

લેપટોપ એ જંગમ ઉપકરણો છે અને નેટવર્ક ધમકીઓ માટે એટલા સંવેદનશીલ છે. એ જ રીતે, મોબાઇલ ફોન વાયરલેસ ઉપકરણો છે અને તે પણ સરળતાથી ધમકીઓ માટે ખુલ્લા છે. આ ઉપકરણોને બચાવવા માટે, તેના વિવિધ સંસાધનોને ઍકસેસ કરવા માટે મજબૂત પાસવર્ડનો ઉપયોગ કરવો જોઈએ. સ્માર્ટ ઉપકરણોને ઍકસેસ કરવા માટે બાયોમેટ્રિક ફિંગર પ્રિન્ટ પાસવર્ડનો ઉપયોગ કરવો વધુ સારું રહેશે.

6. સમયસર બેકઅપ

સમયાંતરે દરેક સિસ્ટમ અથવા હાર્ડ–ડિસ્કમાં ફાઈલો, દસ્તાવેજો અને અન્ય મહત્ત્વપૂર્ણ ડેટાનો બેકઅપ લેવો જોઈએ અને તેને કેન્દ્રિય સર્વર અથવા કોઈ સુરક્ષિત સ્થાન પર સાચવવો જોઈએ. આ હંમેશાં કરવું જોઈએ. કટોકટીના કિસ્સામાં, આ સિસ્ટમને ઝડપથી પુનઃસ્થાપિત કરવામાં મદદ કરશે.

7. વેબસાઇટ્સ પર સ્માર્ટ સર્ફિંગઃ

ઇન્ટરનેટ પર કોઈ પણ લિંક કે સાઈટ પર ડાઉનલોડ અને ક્લિક કરતા પહેલા, આપણે ધ્યાનમાં રાખવું જોઈએ કે એક ખોટી ક્લિક નેટવર્ક પરના ઘણા વાયરસને આમંત્રણ આપી શકે છે, તેથી ફક્ત વિશ્વસનીય અને સુરક્ષિત લિંક્સ પરથી જ ડેટા ડાઉનલોડ કરવું જોઈએ અને અજાણી લિંક્સ અને વેબસાઇટ્સ પર સર્ફિંગ કરવાનું ટાળવું જોઈએ. ઉપરાંત, જ્યારે પણ ઇન્ટરનેટ પર લોગ ઇન કરીયે ત્યારે વેબ–પેજ પર વારંવાર પ્રદર્શિત થતી જાહેરાતો અને ઑફર્સ પર ક્લિક કરવાનું ટાળવું જોઈએ..

8. સુરક્ષિત રૂપરેખાંકનઃ

રાઉટર પર કરવામાં આવેલું કન્ફિગરેશન યુનિક યુઝર આઈડી અને પાસવર્ડનો ઉપયોગ કરીને કરવું જોઈએ અને તેને સુરક્ષિત રાખવું જોઈએ.

9. દૂર કરી શકાય તેવા મીડિયા નિયંત્રણઃ

પેન ડ્રાઈવ, ડોંગલ્સ અને ડેટા કાર્ડ જેવા દૂર કરી શકાય તેવા ઉપકરણો જ્યારે સિસ્ટમમાં પ્રેરિત હોય ત્યારે હંમેશાં સ્કેન કરવા જોઈએ, દૂર કરી શકાય તેવા ઉપકરણોનો ઉપયોગ મર્યાદિત હોવો જોઈએ અને એવી નીતિ બનાવવી જોઈએ કે જેના દ્વારા તે સિસ્ટમમાંથી કોઈપણ ડેટાની નિકાસ ન કરી શકે.

4.4 ઈ-મેલ સુરક્ષા

- **વ્યાખ્યા**

ઈ-મેલ એ એક વિન્ડો છે જેનો ઉપયોગ હેકર્સ તમારી કમ્પ્યૂટર સિસ્ટમમાં પ્રવેશ કરવા માટે કરે છે, જેમ જંતુઓને ઘરમાં પ્રવેશતા અટકાવવા માટે વિન્ડો પર જાળી

લગાવવામાં આવે છે, તેમ તમે તમારા ઇમેઇલ એકાઉન્ટ્સની ઍક્સેસ અને સામગ્રીને સુરક્ષિત કરવા માટે સુરક્ષા સોફ્ટવેર ઇન્સ્ટોલ કરી શકો છો. વ્યક્તિઓ, તેમજ વ્યવસાયિક સંસ્થાઓ, આ સેવાઓનો ઉપયોગ એક અથવા તેમના સમગ્ર એન્ટરપ્રાઇઝ એકાઉન્ટ્સની એકંદર ઍક્સેસને સુરક્ષિત કરવા માટે કરી શકે છે.

- ઈ-મેલ હેકિંગ

ઈ-મેલ હેકિંગ નીચેની કોઈપણ રીતે કરી શકાય છેઃ

1. સ્પામ
2. વાઈરસ
3. ફિશીંગ

ઈ-મેલ સ્પાર્મિંગ અને જંક મેલ્સ

ઈ-મેલ સ્પામિંગ એ અનસોલિસીટેડ બલ્ક ઈ-મેઈલ (UBI) મોકલવાનું એક કાર્ય છે જે માટે કોઈએ પૂછ્યું નથી. ઈ-મેલ સ્પામ એ કોમર્શિયલ કંપનીઓ દ્વારા તેમના ઉત્પાદનો અને સેવાઓની જાહેરાત તરીકે મોકલવામાં આવતી જંક મેઈલ છે.

- **સ્પામ નીચેની સમસ્યાઓનું કારણ બની શકે છે :**

1. તે ઈ-મેઈલ એકાઉન્ટને અનિચ્છનીય ઈ-મેઈલથી ભરી દે છે, જેના પરિણામે જો ઈનબોક્સ ભરાઈ જાય તો મહત્ત્વપૂર્ણ ઈ-મેઈલ ખોવાઈ શકે છે.
2. જંક ઈ-મેલ અથવા સ્પામની સમીક્ષા કરવામાં અને કાઢી નાખવામાં સમય અને શક્તિ વેડફાય છે.
3. તે બેન્ડવિડ્થનો ઉપયોગ કરે છે જે મેઇલની ડિલિવરીની ઝડપને ધીમી કરે છે.
4. કેટલાક અવાંછિત ઈ-મેલમાં વાયરસ હોઈ શકે છે જે તમારા કમ્પ્યૂટરને નુકસાન પહોંચાડી શકે છે.

- **સ્પામ ઘટાડવામાં મદદ કરશેઃ**

1. ન્યૂઝગ્રૂપ અથવા મેઈલિંગ લિસ્ટમાં પત્રો પોસ્ટ કરતી વખતે, અંગત ઈ-મેઈલ માટે જે સરનામું વાપર્યું છે તેના કરતાં અલગ ઈ-મેલ એડ્રેસનો ઉપયોગ કરી શકાય.
2. વેબસાઇટ્સ પર ઇ—મેઇલ સરનામું ન આપવું કારણ કે તે સરળતાથી સ્પામ થઈ શકે છે.
3. અજાણ્યા વ્યક્તિઓ તરફથી મળેલા ઈ-મેલનો જવાબ આપવાનું ટાળવું જોઈએ.
4. પ્રોડક્ટની જાહેરાત કરતા સ્પામના જવાબમાં કયારેય કંઈપણ ન ખરીદવું.

- **ઈ-મેલ સુરક્ષા સુવિધાઓ**

ઈ-મેલ સુરક્ષા સેવાઓ વિવિધ પ્રકારના ઈ-મેલ સુરક્ષા ઉકેલો પ્રદાન કરે છે. કેટલીક મુખ્ય ઇ-મેઇલ સુરક્ષા સુવિધાઓ નીચે મુજબ છે.

1. સ્પામ ફિલ્ટર્સ

દરરોજ મળતા ઇમેઇલ્સમાં નોંધપાત્ર પ્રમાણ માર્કેટિંગ ઇમેઇલ્સ હોઈ છે. આ ઈ-મેલ ઇનબોક્સને એવી રીતે બ્લોક કરે છે કે અમુક ઓફિશિયલ અથવા આવશ્યક ઈ-મેલ લગભગ ચૂકી જવાશે. બીજું, સાયબર અપરાધીઓ તેમના ફિશિંગ ઈ-મેઈલમાં દબાણ

કરીને આ માર્કેટિંગ ઈ-મેલનો લાભ પણ લે છે. અસંદિગ્ધ વપરાશકર્તા આવી ઈ-મેલ ખોલી શકે છે અને ફિશિંગ ઈ-મેલમાં આપેલી દૂષિત લિંક પર ક્લિક કરી શકે છે. તે ગંભીર પરિણામો તરફ દોરી શકે છે જેમ કે કોઇની નાણાકીય વિગતો જેમ કે બેંક ખાતા, ક્રેડિટ કાર્ડ નંબર વગેરે સાથે ચેડા કરવા.

સ્પામ ફિલ્ટર્સ ઇન્સ્ટોલ કરવાથી આ માર્કેટિંગ અને ફિશિંગ ઈ-મેઈલને એક વિશિષ્ટ ઈ-મેલ ઇનબોક્સમાં ડાયરેકટ કરીને અલગ કરવામાં મદદ મળી શકે છે. આ રીતે, નિયમિત ઈ-મેલ ઇનબોક્સ ભરાઈ જતું નથી. બીજું, કોઈપણ નિર્ણાયક વ્યવસાય ઇમેઇલ ચૂકશો નહીં. એક મહત્ત્વપૂર્ણ ઇ-મેઇલ સુરક્ષા સુવિધા એ છે કે તમે નિશ્ચિત સમયાંતરે સ્પામ ઇમેઇલ્સને કાઢી નાખવાનું શેડ્યૂલ કરી શકાય. તેમને ખોલવાની જરૂર વગર આપમેળે કાઢી શકાય છે.

2. એન્ટી વાઈરસ પ્રોટેક્શન

સ્પામ ફિલ્ટર્સ સ્પામ ઈ-મેઈલને નિયમિત રીતે અલગ કરવાની ભૂમિકા ભજવે છે. જો કે, આ ઈ-મેઈલ ચોક્કસ સમયગાળા માટે ઇનબોક્સમાં રહે છે જેના પછી તે આપમેળે ડિલીટ થઈ જાય છે. વપરાશકર્તા સ્પામ ઇ-મેઇલ ઇનબોક્સને ઍક્સેસ કરે છે અને આ ઇ-મેઇલ જોડાણો ખોલે તેની હંમેશાં સંભાવના છે.

હેકર્સ આવા ઈ-મેલ એટેચમેન્ટ્સ અને મેસેજમાં નકલી લિંક્સ દ્વારા દૂષિત સામગ્રી મોકલે છે. જો કોઈ વપરાશકર્તા અજાણતાં આવી લિંક્સ પર ક્લિક કરે છે અથવા આવી ફાઇલો ડાઉનલોડ કરે છે, તો તેમની માહિતી પ્રણાલીમાં વાયરસ ફેલાવાની સંભાવના છે. આવી પરિસ્થિતિઓનો સામનો કરવાનો સાચો રસ્તો એ છે કે મજબૂત એન્ટિ-વાયરસ સુરક્ષા હોય. આ સોફ્ટવેર પ્રોગ્રામ દૂષિત સામગ્રી માટે દરેક ઇનકમિંગ અને આઉટગોઇંગ ઈ-મેઈલને સ્કેન કરે છે અને તેમની એન્ટ્રી અથવા એક્ઝિટને બ્લૉક કરે છે. તેથી, તે સ્પામ ફિલ્ટર્સ કરતાં વધુ સારી સુરક્ષા પ્રદાન કરે છે કારણ કે તે આ વાયરસને ઓળખે છે અને દૂર કરે છે.

3. છબિ (images) અને સામગ્રી નિયંત્રણ

હેકર્સ ફિશિંગ હેતુઓ માટે ઈ-મેલનો ઉપયોગ કરે છે. ઇમેઇલ જોડાણોમાં ફાઇલો, લિંક્સ અને છબિઓ પણ હોઈ શકે છે. તાજેતરના સમયમાં ફિશીંગના અસંખ્ય કિસ્સાઓ છે જ્યાં સાયબર અપરાધીઓ ઈમેજીસ દ્વારા દૂષિત સોફ્ટવેરને ટ્રાન્સમિટ કરવામાં સફળ રહ્યા છે. તેથી, ઈ-મેઈલ સુરક્ષા સેવાઓ માટે ઈમેજીસ સ્કેન કરીને સિસ્ટમનું રક્ષણ કરવું મહત્ત્વપૂર્ણ બની જાય છે. તે માહિતી સુરક્ષામાં ઈ-મેલ સુરક્ષાના સૌથી નિર્ણાયક પાસાઓમાંનું એક છે.

4. ડેટા એન્ક્રિપ્શન

જ્યારે ઈ-મેલ ડેટા ટ્રાન્ઝિટમાં હોય ત્યારે તેની સૌથી વધુ સંવેદનશીલ સ્થિતિમાં હોય છે. સામાન્ય રીતે, તે ખુલ્લા ફોર્મેટમાં પ્રસારિત થાય છે. તે સાયબર અપરાધીઓને આ સંદેશાઓ ટ્રાન્ઝિટમાં અટકાવવા અને ગોપનીય ડેટા ઉપાડવા માટે તેનો ઉપયોગ કરવાની મંજૂરી આપે છે. જ્યારે તમે તમારી ઈ-મેલ સામગ્રી ટ્રાન્ઝિટમાં હોય ત્યારે તેને એક્સપોઝ કરો ત્યારે આ ઈ-મેલ સુરક્ષા સુવિધાઓનો બહુ ઓછો ઉપયોગ થાય છે.

આદર્શ ઉકેલ એ છે કે ઇ-મેઇલ દ્વારા મોકલવામાં આવેલ ડેટાને એન્ક્રિપ્ટ કરવો. તે ક્રિપ્ટોગ્રાફી સિસ્ટમ્સમાં ઈ-મેલ સુરક્ષાને લગતા મહત્ત્વના મુખ્ય વિષયોમાંનો એક છે. આ સુરક્ષા સુવિધા એ સુનિશ્ચિત કરે છે કે તમારી આઉટગોઇંગ ઈ-મેઈલ દરેક રીતે એન્ક્રિપ્ટેડ

ડેટા છે, જેથી હેકરને તેમાં ઘૂસણખોરી કરવાની કોઈ છૂટ આપતી નથી. અદ્યતન ક્રિપ્ટોગ્રાફી સુવિધાઓ પ્રાપ્તકર્તાની વિગતો અને ઈ-મેલ મેસેજ હેડરોના એન્ક્રિપ્શનનું પણ રક્ષણ કરે છે. તેથી, સાયબર અપરાધીઓ પાસે ઈ-મેલની સામગ્રી અથવા પ્રાપ્તકર્તાઓની વિગતો જાણવા માટે કોઈ માધ્યમ નથી. ઈ-મેઈલને એન્ક્રિપ્ટ કરવાથી હેકર્સ માટે ઈ-મેલની સામગ્રીને એક્સેસ કરવામાં મુશ્કેલી પડે છે. દરેક વ્યવસાયિક સંસ્થા એ તેમના કોમ્પ્યૂટર નેટવર્ક પર આ ઈ-મેઈલ સુરક્ષા સુવિધા ઇન્સ્ટોલ કરેલી હોવી જોઈએ. ફિશિંગ પ્રયાસોનો ભોગ બનવાનું ટાળવા માટે તે એક શ્રેષ્ઠ રીત છે.

4.5 વેબ સુરક્ષા

વેબ સુરક્ષા આજકાલ ખૂબ જ મહત્ત્વપૂર્ણ છે. વેબસાઇટ્સ હંમેશાં સુરક્ષાના જોખમોથી ભરેલી હોય છે. વેબ સુરક્ષા ઇન્ટરનેટ/નેટવર્ક અથવા વેબ પર અથવા જ્યારે તે ઇન્ટરનેટ પર ટ્રાન્સફર થઈ રહી હોય ત્યારે ડેટાની સુરક્ષા સાથે વ્યવહાર કરે છે. દા.ત. જ્યારે તમે કલાયંટ અને સર્વર વચ્ચે ડેટા ટ્રાન્સફર કરી રહ્યા હોવ અને તમારે ડેટાને સુરક્ષિત કરવાનો હોય ત્યારે ડેટાની સુરક્ષા તમારી વેબ સુરક્ષા છે.

વેબસાઈટ હેક કરવાથી મહત્ત્વના ગ્રાહકના ડેટાની ચોરી થઈ શકે છે. કદાચ તમારા ક્રેડિટ કાર્ડની માહિતી ગ્રાહકની લૉગિન વિગતો અથવા તે કોઈના વ્યવસાયનો વિનાશ હોઈ શકે છે અને વપરાશકર્તાઓને ગેરકાયદેસર સામગ્રીનો પ્રચાર કરી શકે છે જેથી કોઈ તમારી વેબસાઈટ હેક કરે. ગ્રાહકોની મહત્ત્વપૂર્ણ માહિતીની ચોરી કરી શકે છે અથવા તેઓ તમારી વેબસાઇટ દ્વારા તમારા વપરાશકર્તાઓને ગેરકાયદેસર સામગ્રીનો પ્રચાર પણ કરી શકે છે, તેથી, વેબ સુરક્ષાના સંદર્ભમાં સુરક્ષા વિચારણાઓ જરૂરી છે.

વેબ સુરક્ષા ધમકીઓ :

સુરક્ષા ધમકી એ એક સંભવિત ઘટના સિવાય બીજું કંઈ નથી જે માહિતી પ્રણાલીને નુકસાન પહોંચાડી શકે છે. જ્યારે પણ કોઈ વ્યક્તિ અથવા સંસ્થા વેબસાઈટ બનાવે છે, ત્યારે તેઓ સુરક્ષા હુમલાઓ માટે સંવેદનશીલ હોય છે. સુરક્ષા હુમલાઓનો હેતુ મુખ્યત્વે વ્યક્તિગત અને ગોપનીય માહિતીના ટુકડાને બદલવા અથવા નાશ કરવા, હાર્ડ ડ્રાઈવની જગ્યા ચોરી કરવા, ગેરકાયદેસર રીતે પાસવર્ડ્સ ઍક્સેસ કરવાનો હોઈ છે, તેથી જો તમે બનાવેલ વેબસાઈટ સુરક્ષા હુમલાઓ માટે સંવેદનશીલ હોય તો હુમલાઓ તમારા ડેટાની ચોરી કરે છે, તમારી અંગત માહિતીનો નાશ કરે છે, તમારી ગોપનીય માહિતીને જુએ છે અને તે તમારા પાસવર્ડને પણ એક્સેસ કરે છે.

- **ટોચની વેબ સુરક્ષા ધમકીઓઃ**

વેબ સુરક્ષા ધમકીઓ સતત ઉભરી રહી છે અને વિકસિત થઈ રહી છે, પરંતુ ઘણી બધી ધમકીઓ વેબ સુરક્ષા ધમકીઓની સૂચિની ટોચ પર સતત દેખાય છે. આમાં શામેલ છેઃ

1. ક્રોસ–સાઇટ સ્ક્રિપ્ટીંગ (XSS)
2. એસકયુએલ ઈન્જેકશન (SQL (Structured Query Language) Injection)
3. ફિશીંગ (Phishing)
4. રેન્સમવેર (Ransomware)
5. કોડ ઈન્જેકશન
6. વાયરસ અને વોર્મ્સ
7. સ્પાયવેર
8. સેવાનો ઇનકાર

- **વેબ સુરક્ષા વિચારણાઃ**

1. અપડેટ કરેલ સોફ્ટવેર : હંમેશાં તમારા સોફ્ટવેરને અપડેટ કરતા રહેવું જોઈએ.. હેકર્સ ચોક્કસ સોફ્ટવેરની નબળાઈઓથી વાકેફ હોઈ શકે છે, જે કેટલીકવાર બગ્સને કારણે થાય છે અને તેનો ઉપયોગ તમારી કોમ્પ્યૂટર સિસ્ટમને નુકસાન પહોંચાડવા અને વ્યક્તિગત ડેટાની ચોરી કરવા માટે થઈ શકે છે. સોફ્ટવેરની જૂની આવૃત્તિઓ હેકર્સ માટે નેટવર્કમાં પ્રવેશવાનો ગેટવે બની શકે છે. સૉફ્ટવેર ઉત્પાદકો ટૂંક સમયમાં આ નબળાઈઓથી વાકેફ થઈ જશે અને સંવેદનશીલ અથવા ખુલ્લા વિસ્તારોને ઠીક કરશે. એટલા માટે સૉફ્ટવેરને અપડેટ રાખવું ફરજિયાત છે, તે વ્યક્તિગત ડેટાને સુરક્ષિત રાખવામાં મહત્ત્વપૂર્ણ ભૂમિકા ભજવે છે.

2. એસક્યુએલ ઈન્જેકશનથી સાવચેત રહો : એસક્યુએલ ઈન્જેક્શન એ તમારી ક્વેરી (Query) માં રફ કોડ દાખલ કરીને તમારા ડેટા અથવા ડેટાબેઝને હેરફેર કરવાનો પ્રયાસ છે. દા.ત. કોઈ વેબસાઈટ પર ક્વેરી મોકલે છે જે એક રફ કોડ હોઈ શકે છે. જ્યારે તે એક્ઝિક્યુટ થઈ જાય છે ત્યારે તેનો ઉપયોગ ડેટાબેઝને મેનિપ્યુલેટ કરવા માટે થઈ શકે છે જેમ કે કોષ્ટકો બદલવા, ડેટાને સંશોધિત કરવા અથવા કાઢી નાખવા અથવા તે મહત્ત્વપૂર્ણ માહિતીને પણ પુનઃપ્રાપ્ત કરી શકે છે તેથી, સાવચેત રહેવું જોઈએ.

3. ક્રોસ–સાઈટ સ્ક્રિપ્ટિંગ (XSS) : XSS હુમલાખોરોને વેબ પૃષ્ઠોમાં કલાયંટ–સાઇડ સ્ક્રિપ્ટ દાખલ કરવાની મંજૂરી આપે છે. દા.ત. ફોર્મની રજૂઆત. તે હુમલાઓના વર્ગનું વર્ણન કરવા માટે વપરાતો શબ્દ છે જે હુમલાખોરને વેબસાઈટ દ્વારા અન્ય વપરાશકર્તાઓના બ્રાઉઝર્સમાં ક્લાયંટસાઇડ સ્ક્રિપ્ટ્સ ઈન્જેકટ કરવાની મંજૂરી આપે છે. ઈન્જેકટેડ કોડ સાઈટ પરથી બ્રાઉઝરમાં પ્રવેશે છે, કોડ વિશ્વસનીય છે અને હુમલાખોરને વપરાશકર્તાની સાઈટ અધિકૃતતા કૂકી મોકલવા જેવી વસ્તુઓ કરી શકે છે.

4. ભૂલ સંદેશાઓ : ભૂલ સંદેશાઓ વિશે ખૂબ કાળજી લેવાની જરૂર છે જે વપરાશકર્તાઓને માહિતી આપવા માટે બનાવવામાં આવે છે. જ્યારે વપરાશકર્તાઓ (Users) વેબસાઈટને ઍકસેસ કરે છે ત્યારે કેટલાક ભૂલ સંદેશાઓ એક અથવા બીજા કારણોસર જનરેટ થાય છે. માહિતી પ્રદાન કરતી વખતે ખૂબ કાળજી લેવી જોઈએ. દા.ત. લૉગિન પ્રયાસ - જો વપરાશકર્તા લૉગિન કરવામાં નિષ્ફળ જાય તો ભૂલ સંદેશે વપરાશકર્તાને જણાવવું જોઈએ નહીં કે કયું ક્ષેત્ર ખોટું છેઃ વપરાશકર્તા નામ (User ID) કે પછી પાસવર્ડ.

5. ડેટા માન્યતા : ડેટા માન્યતા એ વપરાશકર્તા અથવા એપ્લિકેશન દ્વારા પૂરા પાડવામાં આવેલ કોઈપણ ઇનપુટનું યોગ્ય પરીક્ષણ છે. તે અયોગ્ય રીતે બનાવેલ ડેટાને માહિતી સિસ્ટમમાં પ્રવેશતા અટકાવે છે. ડેટાની માન્યતા સર્વર-સાઇડ અને કલાયંટ-સાઇડ બંને પર થવી જોઈએ. બંને બાજુએ ડેટા વેલિડેશન કરવું જોઈએ જે પ્રમાણીકરણ આપે. ડેટા માન્યતા ત્યારે થવી જોઈએ જ્યારે કોઈ બહારના પક્ષ તરફથી ડેટા પ્રાપ્ત થાય, ખાસ કરીને જો ડેટા અવિશ્વસનીય સ્ત્રોતોમાંથી હોય.

6. પાસવર્ડ : પાસવર્ડ તમારા ઉપકરણ અને વ્યક્તિગત માહિતીની અનધિકૃત ઍકસેસ સામે સંરક્ષણની પ્રથમ લાઇન પ્રદાન કરે છે. મજબૂત પાસવર્ડનો ઉપયોગ કરવો જરૂરી છે. હેકર્સ ઘણા કિસ્સાઓમાં અત્યાધુનિક સોફ્ટવેરનો ઉપયોગ કરે છે જે પાસવર્ડ ક્રેક કરવા માટે જડ બળ (Brute Force attack)નો ઉપયોગ કરે છે. જડ બળ સામે રક્ષણ આપવા માટે પાસવર્ડ જટિલ હોવા જોઈએ. અપરકેસ અક્ષરો, લોઅરકેસ અક્ષરો, વિશિષ્ટ અક્ષરો અને અંકો સહિત ઓછામાં ઓછા આઠ અક્ષરો લાંબો હોવો જોઈએ જેવી પાસવર્ડ આવશ્યકતાઓને લાગુ કરવી સારી છે.

4.6 Wi-Fi સુરક્ષા

Wi-Fi સુરક્ષા એ વાયરલેસ વાતાવરણમાં જોડાયેલા ઉપકરણો અને નેટવર્કનું રક્ષણ છે. Wi-Fi સુરક્ષા વિના, નેટવર્કિંગ ઉપકરણ જેમ કે વાયરલેસ એકસેસ પોઈન્ટ અથવા રાઉટરને કોમ્પ્યૂટર અથવા મોબાઈલ ડિવાઈસનો ઉપયોગ કરીને કોઈપણ વ્યક્તિ દ્વારા રાઉટરના વાયરલેસ સિગ્નલની રેન્જમાં એકસેસ કરી શકાય છે.

- **અસુરક્ષિત Wi-Fi નેટવકર્સ દ્વારા ઊભું થતું જોખમ :**

જ્યારે નેટવર્કમાં વાયરલેસ ઉપકરણો 'ખુલ્લા' અથવા અસુરક્ષિત હોય છે, ત્યારે તે કોઈપણ Wi-Fi સક્ષમ ઉપકરણ, જેમ કે કોમ્પ્યૂટર અથવા સ્માર્ટફોન, જે તેમના વાયરલેસ સિગ્નલની શ્રેણીમાં હોય છે તેના માટે ઍક્સેસિબલ હોય છે.

ખુલ્લા અથવા અસુરક્ષિત નેટવર્કનો ઉપયોગ વપરાશકર્તાઓ અને સંસ્થાઓ માટે જોખમી હોઈ શકે છે. ઇન્ટરનેટ-કનેક્ટેડ ઉપકરણોનો ઉપયોગ કરતા વિરોધીઓ વપરાશકર્તાઓની વ્યક્તિગત માહિતી એકત્રિત કરી શકે છે અને ઓળખ ચોરી શકે છે, નાણાકીય અને અન્ય સંવેદનશીલ વ્યવસાયિક ડેટા સાથે ચેડા કરી શકે છે.

- **Wi-Fi નેટવર્કને સુરક્ષિત કરવાની પદ્ધતિઓ :**

Wi-Fi સુરક્ષા માટે એક મૂળભૂત શ્રેષ્ઠ પ્રેક્ટિસ નેટવર્ક ઉપકરણો માટે ડિફોલ્ટ પાસવર્ડ્સ બદલવાનો છે. મોટા ભાગના ઉપકરણોમાં ડિફોલ્ટ એડમિનિસ્ટ્રેટર પાસવર્ડ્સ હોય છે, જે ઉપકરણોના સેટઅપને સરળ બનાવવા માટે હોય છે. જો કે, ઉપકરણ ઉત્પાદકો દ્વારા બનાવવામાં આવેલ ડિફૉલ્ટ પાસવર્ડ્સ ઑનલાઇન મેળવવા માટે સરળ હોઈ શકે છે. નેટવર્ક ઉપકરણો માટેના ડિફૉલ્ટ પાસવર્ડ્સને વધુ જટિલ પાસવર્ડ્સમાં બદલવું અને તેને વારંવાર બદલવું-વાઇ-ફાઇ સુરક્ષાને બહેતર બનાવવાની સરળ પણ અસરકારક રીતો છે.

નીચે અન્ય Wi-Fi નેટવર્ક સુરક્ષા પદ્ધતિઓ છે :

1. Media Access Control (MAC) addresses

Wi-Fi સુરક્ષા માટેનો બીજો મૂળભૂત અભિગમ એ NAC સરનામાંનો ઉપયોગ કરવાનો છે, જે Wi-Fi નેટવર્કની ઍક્સેસને પ્રતિબંધિત કરે છે. (એક NAC સરનામું એ એક અનન્ય (unique) કોડ અથવા નંબર છે જેનો ઉપયોગ નેટવર્ક પર વ્યક્તિગત ઉપકરણોને ઓળખવા માટે થાય છે.) જ્યારે આ યુકિત એક ખુલ્લા નેટવર્ક કરતાં ઉચ્ચ સુરક્ષા પ્રદાન કરે છે, તે હજી પણ 'સ્પૂફ' અથવા સંશોધિત સરનામાંનો ઉપયોગ કરીને વિરોધીઓ દ્વારા હુમલો કરવા માટે સંવેદનશીલ છે.

2. એન્ક્રિપ્શન (Encryption)

Wi-Fi નેટવકર્સ અને ઉપકરણોને સુરક્ષિત કરવાની વધુ સામાન્ય પદ્ધતિ એ એન્ક્રિપ્શન છે. ડિજિટલ સંચારમાં એન્ક્રિપ્શન ડેટાને એન્કોડ (Encode) કરે છે અને પછી તેને માત્ર અધિકૃત પ્રાપ્તકર્તાઓ માટે જ ડીકોડ (decode) કરે છે. Wi-Fi પ્રોટેકટેડ એકસેસ (WPA) અને Wi-Fi પ્રોટેક્ટેડ એક્સેસ 2 (WPA2) સહિત અનેક પ્રકારના એન્ક્રિપ્શન ધોરણો આજે ઉપયોગમાં છે.

મોટાભાગના નવા નેટવર્ક ઉપકરણો, જેમ કે એકસેસ પોઈન્ટ અને વાઈ-ફાઈ રાઉટર્સ, બિલ્ટ-ઈન વાયરલેસસિકયોરિટી એન્ક્રિપ્શન પ્રોટોકોલ ધરાવે છે જે Wi-Fi સુરક્ષા પ્રદાન

કરે છે.

3. Virtual private networks (VPNs)

VPN એ Wi-Fi નેટવર્ક સુરક્ષાનો બીજો સ્ત્રોત છે. તેઓ વપરાશકર્તાઓને અસુરક્ષિત Wi-Fi નેટવકર્સ અને ઇન્ટરનેટ વચ્ચે સુરક્ષિત, ઓળખ-સંરક્ષિત ટનલ બનાવવાની મંજૂરી આપે છે.

VPN વપરાશકર્તાના ઇન્ટરનેટ કનેક્શનને એન્ક્રિપ્ટ કરી શકે છે. તે VPN સર્વરમાંથી પસાર થતાં વપરાશકર્તાના ટ્રાફિકને સોંપેલ વર્ચ્યુઅલ IP સરનામાનો ઉપયોગ કરીને વપરાશકર્તાના IP સરનામાને પણ છુપાવી શકે છે.

4. Security Software (સુરક્ષા સોફ્ટવેર)

ઘણા પ્રકારના ગ્રાહક અને એન્ટરપ્રાઇઝ સોફ્ટવેર ઉપલબ્ધ છે જે Wi-Fi સુરક્ષા પણ પ્રદાન કરી શકે છે. Wi-Fi ને સુરક્ષિત કરવા માટે રચાયેલ કેટલાક નવા સોફ્ટવેર સોલ્યુશન્સ ઇન્ટરનેટની Backbone માં Build હોઈ છે અને ક્લાઉડ (Cloud) પ્લેટફોર્મ દ્વારા ઉપલબ્ધ છે. આ સોલ્યુશન્સ વપરાશકર્તાઓને દૂષિત સાઇટ્સને ઍક્સેસ કરવાથી અટકાવીને વાયરલેસ નેટવકર્સના ઉલ્લંઘન સામે સંરક્ષણની પ્રથમ લાઇન પ્રદાન કરે છે.

- **વાયરલેસ સુરક્ષા પ્રોટોકોલના પ્રકાર**

ચાર મુખ્ય વાયરલેસ-સિક્યોરિટી પ્રોટોકોલ છે. આ પ્રોટોકોલ્સ Wi-Fi એલાયન્સ દ્વારા વિકસાવવામાં આવ્યા હતા, જે એક સંસ્થા છે જે વાયરલેસ ટેક્નોલૉજી અને ઇન્ટરઓપરેબિલિટીને પ્રોત્સાહન આપે છે. જૂથે 1990 ના દાયકાના અંતમાં નીચે વર્ણવેલ ત્રણ પ્રોટોકોલ રજૂ કર્યા. ત્યારથી, પ્રોટોકોલ્સને મજબૂત એન્ક્રિપ્શન સાથે સુધારવામાં આવ્યા છે. ચોથો પ્રોટોકોલ 2018માં બહાર પાડવામાં આવ્યો હતો.

1. WEP

પહેલો વાયરલેસ સિક્યુરિટી પ્રોટોકોલ WEP (વાયર્ડ ઇક્વિવેલન્ટ પ્રાઇવસી) હતો. તે 1990 ના દાયકાના અંતથી 2004 સુધી વાયરલેસ નેટવર્ક સુરક્ષા પ્રદાન કરવાની પ્રમાણભૂત પદ્ધતિ હતી. WEP ને ગોઠવવું મુશ્કેલ હતું, અને તે ફક્ત મૂળભૂત (64/128-બીટ) એન્ક્રિપ્શનનો ઉપયોગ કરે છે. WEP હવે સુરક્ષિત માનવામાં આવતું નથી અને નીચે વર્ણવેલ WPA2 જેવા નવા પ્રોટોકોલ દ્વારા બદલવું જોઈએ.

2. WPA

WPA (Wi-Fi પ્રોટેક્ટેડ એક્સેસ) 2003 માં વિકસાવવામાં આવી હતી. તે ટેમ્પોરલ કી ઇન્ટિગ્રિટી પ્રોટોકોલ (TKIP) તરીકે ઓળખાતા સુરક્ષા પ્રોટોકોલનો ઉપયોગ કરીને WEP કરતાં વધુ મજબૂત (128/256-બીટ) એન્ક્રિપ્શન આપે છે. WPA2 સાથે, WPA એ આજે ઉપયોગમાં લેવાતો સૌથી સામાન્ય પ્રોટોકોલ છે. પરંતુ WPA2થી વિપરીત, તે જૂના સોફ્ટવેર સાથે સુસંગત છે,

3. WPA2

WPA2, WPA નું પછીનું સંસ્કરણ, 2004 માં વિકસાવવામાં આવ્યું હતું. એડવાન્સ્ડ એન્ક્રિપ્શન સ્ટાન્ડર્ડ (AES) તરીકે ઓળખાતા સુરક્ષા પ્રોટોકોલનો ઉપયોગ કરીને તેને ગોઠવવાનું સરળ છે અને WPA કરતાં પણ વધુ નેટવર્ક સુરક્ષા પ્રદાન કરે છે. WPA2 પ્રોટોકોલની આવૃત્તિઓ વ્યક્તિગત વપરાશકર્તાઓ અને સાહસો માટે ઉપલબ્ધ છે.

4. WPA3

WPAની નવી પેઢી, જે WPA3 તરીકે ઓળખાય છે, તેના કોઈપણ પુરોગામી કરતાં વધુ સરળ રૂપરેખાંકન અને વધુ મજબૂત (192/256/7384-bit) એન્ક્રિપ્શન અને સુરક્ષા પહોંચાડવા માટે રચાયેલ છે, તે નવીનતમ Wi-Fi 6 નેટવર્ક પર કામ કરવા માટે પણ છે.

- **Wi-Fi નેટવર્ક સુરક્ષા ઉપકરણોના પ્રકાર**

1. સક્રિય ઉપકરણ

વ્યાપારી રીતે ઉપલબ્ધ ઉપકરણોના ઘણા પ્રકારો છે જે પ્રતિકૂળ હુમલાઓ અને અનિચ્છનીય નેટવર્ક ટ્રાફિકને અવરોધિત કરીને નેટવર્ક સુરક્ષા પ્રદાન કરી શકે છે. આ એક પ્રકારને 'સક્રિય' ઉપકરણ તરીકે ઓળખવામાં આવે છે, જે વધારાના નેટવર્ક ટ્રાફિકને અવરોધિત કરવા માટે રૂપરેખાંકિત થયેલ હાર્ડવેર છે. Wi-Fi નેટવર્ક સુરક્ષા માટેના આ ઉપકરણોના ઉદાહરણોમાં ફાયરવોલ, એન્ટિવાયરસ સ્કેનર્સ અને સામગ્રીફિલ્ટરિંગ ઉપકરણોનો સમાવેશ થાય છે.

2. નિષ્ક્રિય ઉપકરણ

નિષ્ક્રિય Wi-Fi નેટવર્ક સુરક્ષા ઉપકરણો અનિચ્છનીય નેટવર્ક ટ્રાફિકને શોધી કાઢે છે અને તેની જાણ કરે છે. નિષ્ક્રિય ઉપકરણો અન્ય Wi-Fi ઉપકરણો કરતા ઓછા પાવરનો ઉપયોગ કરે છે. તેમની પાસે સુરક્ષાનું વધારાનું સ્તર પણ છે કારણ કે તેઓ Wi-Fi રાઉટર્સ સાથે માત્ર ત્યારે જ વાતચીત કરી શકે છે જ્યારે રાઉટર્સ તેમને શોધતા હોય. તે વધારાનું સ્તર મેન-ઇન-ધ-મિડલ (MITM) હુમલાઓને વધુ મુશ્કેલ બનાવે છે. MITM હુમલામાં, પ્રતિસ્પર્ધી તેમની પ્રવૃત્તિને 'સાંભળવા' અથવા તેમની વચ્ચે મુસાફરી કરતા ટ્રાફિકને સંશોધિત કરવા માટે બે પક્ષો વચ્ચેના સંદેશાવ્યવહારને અટકાવવાનો પ્રયાસ કરે છે.

3. નિવારક ઉપકરણ

નિવારક ઉપકરણ, જેમ કે વાયરલેસ ઇન્ટ્રુઝન પ્રિવેન્શન સિસ્ટમ (WIPS), સંભવિત સુરક્ષા સમસ્યાઓ ઓળખવા માટે નેટવર્કને સ્કેન કરી શકે છે. WIPS ને નેટવર્કમાં સંકલિત કરી શકાય છે અથવા એક સેન્સરનો ઉપયોગ કરીને ઓવરલે કરી શકાય છે. કેટલાક WIPS, જો કે, માત્ર તૂટક તૂટક દેખરેખ રાખે છે, જે નેટવર્કને પ્રસંગોપાત્ત સંવેદનશીલ બનાવે છે.

વાયરલેસ સુરક્ષા જોખમો અને જોખમોના ઉદાહરણો

Wi-Fi Users માટે કેટલીક સુરક્ષા સમસ્યાઓ/જોખમો :

Wi-Fi નેટવર્કર્સના વપરાશકર્તાઓને સાયબર ધમકીઓની શ્રેણીના સંપર્કમાં આવવાનું જોખમ રહેલું છે, કારણ કે તેઓ ઇન્ટરનેટ ઍક્સેસ કરવા અને ઑનલાઇન વ્યવહારો કરવા માટે મોબાઇલ ટૅક્નોલૉજીના ઉપયોગને વિસ્તૃત કરે છે. વૈશ્વિક આરોગ્ય કટોકટીએ Wi-Fi સુરક્ષાના મહત્ત્વ પર ભાર મૂકવામાં મદદ કરી છે, કારણ કે ઘણી સંસ્થાઓને હવે તેમના કર્મચારીઓને ઘરેથી કામ કરવાની જરૂર છે. હોમ વાઇ—ફાઇ નેટવર્ક કે જેમાં મજબૂત સુરક્ષા નથી તે હુમલા માટે સંવેદનશીલ હોય છે. આવી નબળાઈ કંપનીના નેટવર્ક્સની સુરક્ષાને જોખમમાં મૂકી શકે છે. સાર્વજનિક Wi-Fiનો પ્રસાર વ્યક્તિગત વપરાશકર્તાઓ અને સંસ્થાઓ માટે સુરક્ષા સમસ્યાઓ પણ બનાવે છે. આ નેટવર્ક્સ વ્યાખ્યા પ્રમાણે 'ખુલ્લા' છે અને તેથી, અસુરક્ષિત છે. સાર્વજનિક નેટવર્કર્સને ઍક્સેસ કરતા ઉપકરણો માલવેર, સ્પાયવેર અને અન્ય દૂષિત પ્રવૃત્તિ માટે અત્યંત સંવેદનશીલ હોય છે, જેમ કે અગાઉ વર્ણવેલ

MITM હુમલા.

નીચે અન્ય પ્રકારની વાયરલેસ સુરક્ષા સમસ્યાઓના થોડા ઉદાહરણો છે.

1. IP સ્પૂફિંગ

હુમલાખોરો વિશ્વસનીય IP સરનામાનો ઢોંગ કરીને વાયરલેસ નેટવર્કમાં પ્રવેશ કરવા માટે IP સ્પૂફિંગનો ઉપયોગ કરે છે. આ અભિગમ હુમલાખોરોને માલવેર રોપવા, ડિસ્ટ્રિબ્યુટેડ-ડિનાયલ-ઓફ-સર્વિસ (DDoS) હુમલાઓ શરૂ કરવા અથવા અન્ય ઘૃણાસ્પદ કૃત્યો કરવા દે છે.

2. DNS-cache poisoning

વાયરલેસ નેટવર્ક્સ DNS પોઈઝનિંગ તરીકે ઓળખાતા જોખમ માટે પણ સંવેદનશીલ હોય છે, જેને ઘણી વખત DNS સ્પૂફિંગ કહેવાય છે. આ યુક્તિમાં નેટવર્કને હેક કરવું અને નેટવર્ક ટ્રાફિકને હુમલાખોરના કમ્પ્યૂટર અથવા સર્વર પર અથવા નેટવર્કની બહારના અન્ય ઉપકરણ તરફ વાળવાનો સમાવેશ થાય છે. વપરાશકર્તાઓ માટે જોખમ એ કાયદેસર નેટવર્કના દૂષિત સંસ્કરણ સાથે કનેક્ટ થવાનું છે જે તેઓ ઍક્સેસ કરવા માગે છે.

3. Piggybacking and wardriving (પિગીબેકિંગ અને વૉર્ડરાઈવિંગ)

અગાઉ નોંધ્યું તેમ, ખરાબ કલાકારો ગેરકાયદેસર પ્રવૃત્તિ, વેબ ટ્રાફિકનું નિરીક્ષણ, માહિતીની ચોરી અને ખુલ્લા અથવા અસુરક્ષિત વાયરલેસ નેટવર્કનો ઉપયોગ કરી શકે છે. તેઓ વાસ્તવિક સબ્સ્ક્રાઈબર્સની ઈન્ટરનેટ સેવા પર 'પિગીબેકીંગ' દ્વારા આ કરી શકે છે. ખરાબ કલાકારો કાયદેસર વપરાશકર્તાઓની જાણ વિના, તેમના પોતાના ઈન્ટરનેટ કનેકશન્સ સેટ કરવા માટે અસુરક્ષિત સેવામાં ટેપ કરે છે.

આ પ્રથાનું બીજું સંસ્કરણ છે, જેને 'વૉર્ડરાઇવિંગ' તરીકે ઓળખવામાં આવે છે. વ્યક્તિઓ વાયરલેસસજ્જ લેપટોપ અથવા સ્માર્ટફોન સાથે ગીચ વસ્તીવાળા વિસ્તારોમાંથી ધીમે ધીમે વાહન અથવા સાયકલ ચલાવે છે, અને કનેકટ કરવા માટે અસુરક્ષિત વાયરલેસ નેટવર્કની શોધ કરે છે. વૉરબાઈકિંગ, વૉરસાઈકલિંગ, વૉરવૉકિંગ અને સમાન અભિગમનો ઉપયોગ કરે છે પરંતુ પરિવહનના અન્ય મોડ્સ સાથે.

પિગીબેકિંગ અને વૉર્ડરાઈવિંગના કિસ્સાઓ ઘણીવાર એવા લોકોના કિસ્સાઓ છે કે જેઓ ફક્ત 'મફત' ઈન્ટરનેટ કનેકશન શોધી રહ્યા છે, ત્યાં ચોક્કસપણે પ્રશ્ન છે કે શું આ પ્રથાઓ નૈતિક છે. અને ઘણી વ્યક્તિઓ કે જેઓ આ પ્રવૃત્તિઓમાં જોડાય છે તેઓ તોફાન કરવાના ઈરાદા ધરાવે છે. એટલા માટે Wi-Fi સુરક્ષા એ વાઇ-ફાઇ નેટવર્કના તમામ વપરાશકર્તાઓ માટે મનની ટોચની ચિંતા હોવી જોઈએ.

4.7 તમારી પ્રગતિ ચકાસો

---

1. નેટવર્ક સુરક્ષા શું છે અને એનું મહત્ત્વ સમજાવો.

____

____

____

____

____

____

2. ઈ–મેઈલ સ્પામિંગ ના લીધે થનારી સમસ્યાઓ જણાવો.

3. વાયરસ અને વોર્મ વચ્ચેનો તફાવત સમજાવો.

4. સુરક્ષા સિદ્ધાંતો વિષે સમજૂતી આપો.

5. તમારી સિસ્ટમ અને નેટવર્કને સુરક્ષિત કરવાના ઉપાયો જણાવો.

6. ફિશિંગ એન્ડ રેન્સમવેર સમજાવો.

7. અસુરક્ષિત વાઈફાઈ નેટવર્ક કેવી રીતે જોખમી છે અને તેને સુરક્ષિત કરવાની કેટલીક રીતો સમજાવો.

4.8 ચાવીરૂપ શબ્દો

- **વાઈફાઈ નેટવર્ક :** વાયરલેસ નેટવર્ક એક પ્રકારનું નેટવર્ક છે જેમાં ડેટાને વાયર અથવા કેબલનો ઉપયોગ કર્યા વગર એક ઉપકરથી બીજા ઉપકરણમાં મોકલવામાં આવે છે. આ ન્ટવર્કનો ઉપયોગ ઘરો, ઑફિસો અને જાહેર સ્થળોએ ઇન્ટરનેટ કનેક્શન શેર કરવા માટે થાય છે.
- **ઈ-મેઈલ સ્પામીંગ :** ઈ-મેઈલ સ્પામીંગ એ એક પ્રકારનો સાયબર અપરાધ છે જેમાં ઈ-મેઈલો મોટી સંખ્યામાં લોકોને મોકલવામાં આવે છે. આ ઈ-મેઈલોમાં સામાન્ય રીતે જાહેરાતો, ઠગાઈ અથવા વાયરસ હોય છે.
- **સુરક્ષા ધમકી :** સુરક્ષા ધમકી એ એકપણ વ્યક્તિ, સંસ્થા અથવા સિસ્ટમને નુકસાન પહોંચાડવાની ક્ષમતા ધરાવતો કોઈપણ કાર્ય અથવા ઘટના છે.
- **નેટવર્ક સુરક્ષા :** નેટવર્ક સુરક્ષા એ એક પ્રકારની સુરક્ષા છે જેનો ઉપયોગ અનધિકૃત ઍક્સેસ, ઉપયોગ, વિક્ષેપ, પરિવર્તન અથવા વિનાશથી નેટવર્કને સુરક્ષિત રાખવા માટે થાય છે.
- **એન્ટી વાયરસ પ્રોટેક્શન :** એન્ટી વાયરસ પ્રોટેક્શન એ એક પ્રકારનું સોફ્ટવેર છે જેનો ઉપયોગ કમ્પ્યૂટર વાયરસ, વોર્મ્સ, ટ્રોજન હોર્સ અને અન્ય માલવેરથી સુરક્ષિત રાખવા માટે થાય છે.

4.9 સંદર્ભસૂચી

- Juanita Ellis, Tim Speed, William P. Crowell, " The Internet Security Guidebook: From Planning to Deployment," Academic Press, February 2001, 375 pages.
- Jon C. Graff, " Cryptography and E-Commerce: A Wiley Tech Brief," Wiley, December 2000, 208 pages.
- Cryptography and Network Security |4th Edition.- Atul Kahate, McGrow Hill
- Information Systems Security, Godbole, Wiley-India
- Information Security Principles and Practice, Deven Shah, Wiley-India
- Security in Computing by Pfleeger and Pfleeger, PHI

એકમ-5 સોશિયલ મીડિયા અને સાયબર સુરક્ષા

: રૂપરેખા :

5.0 ઉદ્દેશ

5.1 સોશિયલ મીડિયાસાયબર એટેક વેક્ટર તરીકે

5.2 વિવિધ પ્રકારના સોશિયલ મીડિયા હુમલાઓ

5.3 ફેક પ્રોફાઈલ

5.4 સોશિયલ એન્જિનિયરિંગ

5.5 બનાવટી રૂપરેખા

5.6 રૂપરેખા સમાધાન

5.7 દુષ્ટ સામગ્રી

5.8 ડિજિટલ જોખમને ડિજિટલ સંરક્ષણની જરૂર

- **સારાંશ**

5.9 તમારી પ્રગતિ ચકાસો

5.10 ચાવીરૂપ શબ્દો

5.11 ઉપયોગી પુસ્તકોની યાદી

5.0 ઉદ્દેશ

વિદ્યાર્થી મિત્રો, આ પ્રકરણનો અભ્યાસ કર્યા બાદ તમે;

- સોશિયલ મીડિયા દ્વારા થતા વિવિધ હુમલાના પ્રકારો વિષે જાણી શકશો.
- હુમલાખોરો દ્વારા થતા વિવિધ સાયબર હુમલાને કેવી રીતે ટાળી શકીએ તે અંગે માહિતી પ્રાપ્ત કરશો.
- વિવિધ પ્રકારના ડિજિટલ જોખમને ડિજિટલ સંરક્ષણ વિષે જાણશો.

5.1 સોશિયલ મીડિયાસાયબર એટેક વેક્ટર તરીકે

સાયબર સિક્યોરિટીમાં હુમલાખોર સીસ્ટમ, નેટવર્ક, વ્યક્તિ અથવા સંસ્થાની નબળાઈ શોધવા માટે જે અલગ અલગ પ્રકારની રીતો કે માધ્યમોનો ઉપયોગ કરે છે તેને એટેક વેક્ટર કહેવામાં આવે છે. આજના સમયમાં સંદેશાવ્યવહાર માટે સોશિયલ મીડિયા નેટવર્ક એક મહત્ત્વપૂર્ણ માધ્યમ છે. તેના દ્વારા લોકો એક બીજા સાથે ખૂબ જ ઝડપથી અને આકર્ષક રીતે માહિતીઓનું આદાન-પ્રદાન કરી શકે છે. આ જ કારણથી વિશ્વમાં આજે મોટાભાગના લોકો સોશિયલ મીડીયાના માધ્યમથી એક-બીજા સાથે જોડાયા છે. ટ્વિટરનું માઈક્રોબ્લોગિંગ પ્રસારણ હોય કે ફેસબુકનું રિલેશનશીપ-હબ પોર્ટલ, કે પછી વોટ્સએપની સ્પોર્ટ્સ કલબ, લાખો લોકોએ પોતાના વિશેની ઘણીખરી માહિતી વિવિધ સોશિયલ મીડિયા માધ્યમો પર અપલોડ કરી છે અને હજુ પણ કરી રહ્યા છે.

આજનો સોશિયલ મીડિયાનો એક સામાન્ય વપરાશકર્તા પોતાના વિવિધ ફોટોથી લઈને, પોતે ખરીદેલા કપડાં, પોતાના જીવનમાં બનેલા વિવિધ પ્રસંગો, પોતે જોયેલા સ્થળો,

પરિવારના સભ્યો અને ઘરમાં યોજાતા પ્રસંગો વગેરે જેવી બધી જ સંવેદનશીલ માહિતી વિવિધ સોશિયલ મીડિયા માધ્યમો પર મૂકે છે. જો કોઈ વ્યક્તિ ખરાબ આશયથી આ માહિતીનો ઉપયોગ કરે તો તે વપરાશકર્તાને ખૂબ જ મોટું નુકસાન પહોંચાડી શકે છે. આ જ કારણથી જો હુમલાખોરો સોશિયલ મીડીયાને સાયબર એટેક માટેના એક મહત્ત્વના માધ્યમ તરીકે જુવે છે. ભૂતકાળમાં એવા કેટલાક પ્રસંગો બન્યા છે કે જેમાં કોઈ સોશિયલ મીડીયા માધ્યમ પર રહેલી હજારો લોકોની માહિતી હુમલાખોરોએ ચોરી લીધી હોય.

સોશિયલ નેટવર્કિંગ સાઈટ્સ વપરાશકર્તા માટે ખતરારૂપ

- **ગોપનીયતા ઉજાગર કરે છે :** આજે ગૂગલ સર્ચ એન્જિનમાં એવી ક્ષમતાઓ છે કે તે સોશિયલ નેટવર્કિંગ એકાઉન્ટ ધરાવતા કોઈપણ વ્યક્તિને સરળતાથી શોધી શકે છે. ધારો કે કોઈ યુટ્યુબરે પોતાની ચેનલ પર કેટલીક માહિતી મૂકેલી છે અને કોઈને તેના વિષે વિશેષ માહિતી જણાવી છે તો તે વ્યક્તિ આ યુટ્યુબરની બીજી માહિતી મેળવવા માટે ફેસબુક, ટ્વીટર, લિન્કડીન વગેરે જેવા બીજા સોશિયલ મીડિયા માધ્યમનો ઉપયોગ કરશે. યુટ્યુબરે પણ પોતાની પ્રસિદ્ધિ માટે અને વધુમાં વધુ લોકો પોતાની સાથે જોડાય તે માટે દરેક લોકો પોતાની માહિતી જોઈ શકે તેવું રાખ્યું છે. આવા કિસ્સામાં પોતાની માહિતીની ગોપનીયતા લગભગ અશકય છે અને જે સાયબર હુમલાખોરોને પોતાના તરફ આકર્ષે છે.
- **ચહેરાને ઓળખ આપે છે :** ફેસબુક અને ઈન્સ્ટાગ્રામ જેવી સોશિયલ નેટવર્કિંગ સાઈટ્સ પોતાના પોર્ટલ પર અપલોડ થયેલા ફોટોમાં કોણ છે તે જાણવા અને બીજા લોકોને તે માહિતી મોકલવા માટે ચહેરાની ઓળખ કરે છે. તેઓ મૂળભૂત રીતે લોકોના ફોટાને તેમના એકાઉન્ટ સાથે લિંક કરે છે અને પછી તેનો ઉપયોગ લોકોને સજેશન આપવા માટે કરે છે.
- **વ્યક્તિને ઓળખાવવામાં મદદરૂપ થાય છે :** ઈન્સ્ટાગ્રામ પર લોકો જ્યાં ઈમેજ લેવામાં આવી હોય તે જીપીએસને ટેગ કરે છે, તેઓ તેમના સાથી ઈન્સ્ટાગ્રામ વપરાશકર્તાઓની પ્રોફાઈલને ટેગ કરે છે અને અંતે તેઓ રસના વિષયોને ટેગ કરે છે જેને 'હેશટેગ્સ' તરીકે પણ ઓળખવામાં આવે છે. આ ડેટા હુમલાખોરને વ્યક્તિના સમયપત્રક, શોખ અને આદતોને સમજવામાં ખૂબ મદદ કરે છે અને ઘણાબધા પ્રશ્નોના જવાબો આપી દે છે.

ઉપર જોયેલા મુદ્દાઓથી આપણે ચોક્કસપણે કહી શકીએ કે જો સોશિયલ મીડિયાનો સાવધાનીપૂર્વક ઉપયોગ કરવામાં ન આવે તો તે વપરાશકર્તા માટે ખતરારૂપ બની શકે છે. હુમલાખોરો આ માધ્યમનો દુરુપયોગ કરીને નીચે મુજબના હુમલા કરી શકે છે.

5.2 વિવિધ પ્રકારના સોશિયલ મીડિયા હુમલાઓ

સોશિયલ મીડિયા વિવિધ પ્રકારના હુમલાઓ માટે સંવેદનશીલ છે. નીચે સાયબર ગુનેગારો દ્વારા કેટલાક સૌથી વધુ પ્રેકિટસ કરાયેલા સાયબર હુમલાઓની માહિતી આપેલી છે.

1. **નકલી પ્રોફાઈલ :** કોઈ વ્યક્તિની, અધિકૃત ન હોય તેવા વ્યક્તિ દ્વારા સોશિયલ મીડિયામાં પ્રોફાઈલ બનાવવામાં આવે તેને નકલી સોશિયલ મીડિયા પ્રોફાઈલ કહેવામાં આવે છે. નકલી સોશિયલ મીડિયા પ્રોફાઈલનો ઉપયોગ નાના અને મોટા પાયે સાયબર હુમલા કરવા માટે થાય છે. ઘણીવખત નકલી પ્રોફાઈલ્સનો ઉપયોગ સામૂહિક માલવેર અથવા ફિશિંગ વેબસાઈટને જે તે વ્યક્તિના ફોલોવર્સ અને તેમના સંપર્કો સુધી પહોચાડવા થાય છે. વળી કેટલીકવાર વ્યક્તિના ફોલોવર્સ અથવા તો તેના સંપર્કમાં રહેલા લોકો પાસેથી કોઈ માહિતી કઢાવવા માટે પણ નકલી પ્રોફાઈલનો

ઉપયોગ થાય છે. ઉદાહરણ તરીકે, કોઈ કંપનીના CEOની નકલી પ્રોફાઇલનો ઉપયોગ કરીને, આ સાયબર અપરાધીઓ કંપની વિશે વ્યક્તિગત અથવા સંવેદનશીલ માહિતી માટે પૂછી શકે છે અથવા તો તેઓ કર્મચારીને એવું કંઈક કરવા માટે પણ સૂચના આપી શકે છે જે વ્યવસાયની કામગીરીમાં ખલેલ પહોંચાડી શકે. કોઈ વખત આ હુમલાખોરો વ્યક્તિની નકલી પ્રોફાઈલ દ્વારા પૈસાની માંગણી પણ કરી શકે છે.

2. **ચેડાં કરાયેલ પ્રોફાઇલ :** જ્યારે કોઈ વગદાર વ્યક્તિ અથવા બ્રાન્ડની સોશિયલ મીડિયા પ્રોફાઈલને હેક કરવામાં આવે છે ત્યારે તેને ચેડા કરાયેલ પ્રોફાઈલ (પ્રોફાઈલ સમાધાન) કહે છે. બ્રાંડના ગ્રાહકોને અથવા વ્યક્તિના સંપર્કમાં રહેલા લોકોને દૂષિત સામગ્રીના સંપર્કમાં લાવવા માટે ચેડા કરાયેલ પ્રોફાઇલનો ઉપયોગ કરી શકાય છે. આ હુમલો બ્રાન્ડ હાઈજેકિંગ જેવો જ છે અને તે ખૂબ જ નુકસાનકારક હોઈ શકે છે કારણ કે તે સંસ્થાની વેબસાઈટ પર પણ નકારાત્મક અસર કરી શકે છે. 2018માં એક પ્રખ્યાત બ્રાન્ડની પ્રોફાઈલને હેક કરવામાં આવેલ અને ત્યારબાદ આ ચેડાં કરાયેલ પ્રોફાઇલનો ઉપયોગ ગ્રાહકોને ખોટી અને લોભામણી સ્કીમમાં જોડાવા માટે બિટકોઈન સબમિટ કરવા પ્રોત્સાહિત કરવા માટે કરવામાં આવ્યો હતો.

3. **દૂષિત લિંક અને સામગ્રી :** ઘણીવખત દૂષિત સામગ્રી સીધી સોશિયલ મીડિયા પ્લેટફોર્મ પર પોસ્ટ કરવાને બદલે, સાયબર અપરાધીઓ લોકોને આકર્ષક લાગે તેવી માહિતીની સાથે દુષિત લિંકનું જોડાણ કરી દે છે જેથી જ્યારે કોઈ વ્યક્તિ તે આકર્ષક લાગતી માહિતી જોવા માટે તેની સાથે જોડાયેલ દુષિત લીંક ઉપર કિલક કરે ત્યારે તે દૂષિત સામગ્રી કિલક કરનાર વ્યક્તિની પ્રોફાઈલ અથવા તો તે વ્યક્તિ જે યંત્ર વાપરે છે તેને દૂષિત કરે છે.

4. **સોશિયલ એન્જિનિયરિંગ :** સાયબર અપરાધીઓ આ પ્રકારના હુમલાને અંજામ આપવા માટે વ્યક્તિઓના માનસિક વલણ અને ડર, આનંદ, લાલચ વગેરે જેવી લાગણીઓનો ઉપયોગ કરે છે. દા. ત. ઘણીવાર આપણા ઈ-મેઈલ એકાઉન્ટમાં લોભામણા મેઈલ આવતા હોય છે કે જેમાં જણાવવામાં આવે છે કે આપણને કોઈ લોટરી લાગી છે અથવા તો કોઈ સ્કીમ માટે આપણી પસંદગી થઇ છે કે જેમાં આપણને અમુક રૂપિયા મળવા પાત્ર છે અને તેના માટે આપણે આપણી કેટલીક માહિતી અમુક લીંક ઉપર આપવાની છે. આવા પ્રકારના મેસેજ જોવા માટે ઘણા લોકો લલચાય જાય છે અને હુમલાનો ભોગ બને છે. હુમલાખોરો ચોકકસ વ્યક્તિના સોશિયલ મીડિયા એકાઉન્ટની જાસૂસી કરી તેમાંથી મળેલ માહિતીને આધારે તે વ્યક્તિને અનુરૂપ કાયદેસર દેખાય તેવા ખોટા ઈમેઇલ્સ અથવા સંદેશા બનાવી સાયબર હુમલો કરે છે.

5. **સોશિયલ મીડિયા એકાઉન્ટની જાસૂસી :** મોટાભાગે હુમલાખોર વાસ્તવિક હુમલો કરતા પહેલા જે વ્યક્તિ ઉપર સાયબર હુમલો કરવો હોય તેના વિશેની તમામ સંભવિત માહિતી એકત્ર કરવા માટે તેના સોશિયલ મીડિયા એકાઉન્ટની જાસૂસી કરે છે. આજના યુગમાં સોશિયલ મીડિયાની લોકપ્રિયતાને કારણે લોકો પોતાની ઘણીબધી માહિતી સોશિયલ મીડિયા એકાઉન્ટ ઉપર વારંવાર મૂક્તા હોય છે જેમ કે પોતાના પરિવારના સભ્યોના ફોટા, પોતે કોઈ જગ્યા એ ફરવા ગયા હોય તેની વિગત, પોતાના ઘરે ઉજવાયેલ પ્રસંગનાં ફોટા વગેરે. સાયબર હુમલાખોરો યુઝર્સની પ્રોફાઈલની જાસૂસી કરી તેમાં જે પણ માહિતી ઉપલબ્ધ હોય તેનું વિશ્લેષણ કરી જે તે વ્યક્તિની માનસિકતા અને રસ રુચી જાણીલે છે અને તેના આધારે સાયબર હુમલો કરે છે. વળી આ માહિતીનો ઉપયોગ ઓનલાઈન બેંકિંગ જેવી અન્ય સેવાઓ અથવા એકાઉન્ટ્સને પ્રમાણિત કરવા અથવા ઍક્સેસ કરવા માટે કરી શકે છે. કોઈપણ એકાઉન્ટની જાસૂસી

સોશિયલ મીડિયા પર નિષ્ક્રિય રહીને પણ કરી શકાય છે અને એટલે જ હુમલાખોર કોઈના એકાઉન્ટની જાસૂસી કરી રહ્યું છે કે કેમ તેને શોધવું મુશ્કેલ છે.

6. **ફિશિંગ :** આ પ્રકારના હુમલામાં વિવિધ સોશિયલ મીડિયા પ્લેટફોમ જેવા કે ઈન્સ્ટાગ્રામ, લિંકડઇન, ફેસબુક, ટ્વિટરની તેમના જેવી જ દેખાતી નકલી વેબસાઈટ અથવા મોબાઈલ એપ બનાવવામાં આવે છે. આ નકલી વેબસાઈટ અથવા મોબાઈલ એપની URL અથવા નામ વાસ્તવિક વેબસાઈટ કે મોબાઈલ એપ જેવા જ હોય છે, તેમાં માત્ર એક કે બે અક્ષરોનો જ તફાવત હોય છે જે મોટાભાગના વપરાશકર્તાઓને પ્રથમ દ્રષ્ટિએ નજરમાં આવતો નથી. જ્યારે કોઈ વ્યક્તિ નકલી વેબસાઈટ અથવા એપમાં લોગિન કરવા માટે પોતાનો User Id અને પાસવર્ડ પ્રદાન કરે છે, ત્યારે હુમલાખોર સુધી તે વ્યક્તિના User Id અને પાસવર્ડ પહોંચી જાય છે અને તે હુમલાખોર હવે તે વ્યક્તિના પ્રમાણિત એકાઉન્ટનો ઉપયોગ ધારે તે રીતે કરી શકે છે.

સોશિયલ મીડિયાનો ઉપયોગ કરી હુમલો કેવી રીતે થાય છે ?

સોશિયલ મીડિયાનો ઉપયોગ કરી જે હુમલા કરવામાં આવે છે તે નીચે મુજબના તબક્કાઓમાં વિભાજીત કરવામાં આવે છે.

1. ફૂટપ્રિન્ટિંગઃ જે વ્યક્તિ અથવા સંસ્થા ઉપર સાયબર હુમલો કરવામાં આવે છે તેને સાયબર સિક્યોરિટીની ભાષામાં ટાર્ગેટ કે લક્ષ્ય કહેવાય છે. આ ટાર્ગેટ અંગેની શક્ય તેટલી વધુ માહિતી મેળવી તેની નબળાઈઓ જાણવા માટેની ક્રિયાને ફૂટપ્રિન્ટિંગ કહેવામાં આવે છે. આ માહિતીનો ઉપયોગ લક્ષ્ય પર હુમલા કરવા માટે થઈ શકે છે. આ જ કારણે આ તબક્કાને પ્રિ-એટેક નામ પણ આપવામાં આવ્યું છે. ફૂટપ્રિન્ટિંગ કરવા માટે સક્રિય અને નિષ્ક્રિય એમ બંને પ્રકારની રીતો ઉપલબ્ધ છે.

નિષ્ક્રિય ફૂટપ્રિન્ટિંગમાં લક્ષ્યના સીધા સંપર્કમાં આવ્યા વગર જ હુમલાખોરો તેના વિશેની માહિતી એકઠી કરે છે. સોશિયલ મીડિયા, વેબસાઈટ, ઓનલાઈન ડિરેક્ટરી વગેરે માંથી લક્ષ્ય અંગેની માહિતી લેવી તે નિષ્ક્રિય ફૂટપ્રિન્ટિંગની કેટલીક રીતો છે. ફૂટપ્રિન્ટિંગની સક્રિય રીતમાં હુમલાખોર કોઈના કોઈ માધ્યમ દ્વારા લક્ષ્યના સીધા સંપર્કમાં આવી તેના અંગેની માહિતી એકઠી કરે છે. પોર્ટ સ્કેનિંગ અને વનરેબિલિટી સ્કેનિંગ માટેના વિવિધ સોફટવેરનો ઉપયોગ કરી સક્રિય રીતે ફૂટપ્રિન્ટિંગ કરી શકાય છે.

આ તબક્કા દરમ્યાન લક્ષ્ય પાસે કઈ ઓપેરેટિંગ સિસ્ટમ છે, તેના નેટવર્કનું માળખું કેવું છે, તેની પાસે કયા સોફટવેર ઈન્સ્ટોલ કરેલા છે વગેરે જેવી વિવિધ પ્રકારની માહિતી હુમલાખોરો એકઠી કરે છે અને તેનાં દ્વારા લક્ષ્યના નબળા પાસાઓ ઓળખી હુમલા વખતે તેનો ઉપયોગ કરે છે.

2. **મોનિટરિંગ :** સોશિયલ મીડિયા મોનિટરિંગ એ હુમલાખોરે નક્કી કરેલા લક્ષ્ય વિશે વિવિધ સ્ત્રોત દ્વારા શું કહેવામાં આવે છે તે જાણવાની પ્રક્રિયા છે. સોશિયલ મીડિયા મોનિટરિંગ એ અલ્ગોરિધમ આધારિત સાધન છે જે વેબસાઈટ જેવા સ્ત્રોતને ક્રોલ કરે છે અને તેમાંથી પ્રશ્નો અથવા કીવર્ડને આધારે માહિતી શોધી કાઢે છે. જ્યારે જ્યારે લક્ષ્યને અનુલક્ષીને કોઈપણ માહિતી મૂકાય ત્યારે ક્રોલિંગની મદદથી તરત જ તે માહિતી હુમલાખોર સુધી પહોંચી જાય છે.

3. **નકલી પ્રોફાઈલ બનાવવી/પ્રોફાઈલ હેક કરવી :** આ તબક્કામાં હુમલાખોર હુમલો કરતા પહેલા લોકોનો વિશ્વાસ સ્થાપિત કરવા માટે લક્ષ્યની નકલી પ્રોફાઇલ બનાવે છે અને તેના સંપર્કમાં આવી શકે તેવા લોકોને આ નકલી પ્રોફાઈલ સાથે જોડવા

માટે વિનંતી કરે છે. કેટલાક કિસ્સાઓમાં વપરાશકર્તાઓની પ્રોફાઈલ ગેસિંગ, કોડિંગ, ફિશિંગ વગેરે જેવી રીતોનો ઉપયોગ કરી હેક કરી લેવામાં આવે છે જેના દ્વારા હુમલાખોર પાસે તે લક્ષ્યની પ્રોફાઈલનો સંપૂર્ણ કંટ્રોલ આવી જાય છે.

4. **હુમલો :** આ અંતિમ તબક્કામાં હુમલાખોર, બનાવેલી નકલી પ્રોફાઈલ દ્વારા અથવા તો હેક કરેલી પ્રોફાઈલ દ્વારા વિવિધ પ્રકારના સાયબર હુમલા કરે છે જેમ કે સોશિયલ એન્જિનિયરિંગ માટે પ્રોફાઈલનો ઉપયોગ, દૂષિત લિંક અથવા દુષિત માહિતી ફેલાવવા, વ્યક્તિ અથવા સંસ્થાને બદનામ કરવા અને ઘણું બધું.

5.3 બનાવટી રૂપરેખા (Fake Profile)

ફેક પ્રોફાઈલ શું છે ?

સોશિયલ મીડિયા પર વ્યક્તિ અથવા કંપનીની જાણ બહાર તેનું પ્રતિનિધિત્વ કરવા માટે હુમલાખોરો દ્વારા અનઅધિકૃત રીતે તૈયાર કરવામાં આવેલી પ્રોફાઈલને ફેક અથવા તો નકલી પ્રોફાઈલ કહે છે. કોઈ પ્રતિષ્ઠિત વ્યક્તિ અથવા તો કંપનીની ફેક પ્રોફાઈલ બનાવી લોકોને ગેરમાર્ગે દોરવામાં આવે છે. આ ઉપરાંત ચોક્કસ લોકો અને લક્ષ્યાંકિત પ્રેક્ષકોને આકર્ષવા માટે પણ ફેક પ્રોફાઈલ ડિઝાઈન કરવામાં આવે છે. ઘણીવાર કોઈ આકર્ષક મહિલા કે પુરુષના ફોટા સાથે તેની ફેક પ્રોફાઈલ તૈયાર કરવામાં આવે છે જેથી વધુમાં વધુ લોકો આ ફેક પ્રોફાઈલ સાથે જોડાય અને હુમલાનો શિકાર બને.

ફેક પ્રોફાઇલનો ઉપયોગ કોણ કરે છે ?

નકલી પ્રોફાઇલનો ઉપયોગ કરવો એ અનૈતિક છે, પરંતુ દૂષિત ઈરાદો ધરાવતા લોકો તેનો ઉપયોગ વિવિધ હેતુઓ માટે કરી શકે છે, જેમાં નીચેનાનો સમાવેશ થાય છેઃ

- **સ્કેમર્સ :** એવા હુમલાખોરો કે જે લોકોને છેતરી તેમની પાસેથી પૈસા અથવા તો વ્યક્તિગત માહિતી મેળવવા માટે નકલી પ્રોફાઇલનો ઉપયોગ કરે છે તેને સ્કેમર કહેવામાં આવે છે.
- **કેટફિશર્સ :** આ પ્રકારના લોકો પોતાની સાથે વધુમાં વધુ લોકો જોડાઈ તેના માટે પોતાની ખોટી અને આકર્ષક પ્રોફાઈલ બનાવતા હોય છે. ત્યારબાદ તેઓ પોતાની સાચી ઓળખ છુપાવી તેમની સાથે જોડાયેલા લોકોને છેતરે છે અને એક વિકૃત આનંદની અનુભૂતિ કરે છે.
- **સાયબરબુલિઝ :** આ પ્રકારના લોકો અન્ય લોકોને ઓનલાઈન હેરાન કરવા અથવા ડરાવવા માટે નકલી પ્રોફાઇલનો ઉપયોગ કરી શકે છે.
- **ટ્રોલ્સ :** આ પ્રકારના લોકો કોઈ વિવાદ કે મુદ્દાનો પ્રચાર કરવા અથવા અન્ય લોકોને કોઈ પ્રસંગને અનુલક્ષીને તીવ્ર ભાવનાત્મક પ્રતિક્રિયાઓ આપવા ઉશ્કેરવા માટે નકલી પ્રોફાઇલ બનાવે છે.

ફેક પ્રોફાઈલને કેવી રીતે ઓળખવી ?

નીચે જણાવેલ મુદ્દાઓને ધ્યાનમાં રાખવાથી ફેક પ્રોફાઇલને ઓળખવા માટે મદદ મળે છે.

- પ્રોફાઈલમાં બહુ ઓછા ફોટા છે અથવા તો કોઈ ફોટો જ નથી.
- પ્રોફાઈલ તાજેતરમાં અથવા તો થોડા વખત પહેલાં જ બનાવેલ હોય.
- પ્રોફાઈલમાં કોઈ સમાન સંપર્કો ન હોય અથવા તો ખૂબ જ ઓછા સમાન સંપર્કો હોય.
- જો કોઈ પ્રોફાઇલ તમને એડ કરે છે પરંતુ તે પ્રોફાઇલ સાથે તમારો કોઈ સંપર્ક

કે સંબંધ નથી તો તે પ્રોફાઇલ ફેક હોય શકે છે. આવી પ્રોફાઈલનો ઉપયોગ કરનાર વ્યક્તિને જે જોઈએ છે તે તેને મેળવી લીધું હશે પછી તે તમારી સાથે વાત કરવાનું ટાળશે.

ફેક પ્રોફાઈલની કેટલીક ઘટનાઓ :

- રાજસ્થાનમાં એક 16 વર્ષના છોકરાને ચેંગલપટ્ટુ જિલ્લા કલેક્ટરની ફેક ફેસબુક પ્રોફાઇલ બનાવવાના આરોપમાં પકડવામાં આવ્યો હતો. તે કલેક્ટર તરીકે તેમના જિલ્લાની મદદના બહાને લોકો પાસેથી પૈસા માંગતો હતો અને તેમાંથી ઘણાએ તેને પૈસાની મદદ પણ કરી હતી.
- દિલ્હીમાં એક વ્યક્તિની તેની સહકર્મીનું ફેક સોશિયલ મીડિયા એકાઉન્ટ બનાવવા અને તે નકલી પ્રોફાઇલમાંથી તેણીના કોન્ટેક પર અપમાનજનક સંદેશા મોકલવા બદલ ધરપકડ કરવામાં આવી હતી. આ બધું તે વ્યક્તિ એ તેણી સાથે બદલો લેવાની ભાવનાથી કર્યું.

ફેક પ્રોફાઈલ્સ સામે રક્ષણ માટે સારી ઓનલાઈન પ્રથાઓ :

- તમારી વ્યક્તિગત માહિતી જેમ કે સરનામું, મોબાઈલ ફોન નંબર, વ્યક્તિગત ઈમેલ આઈડી અને અન્ય સંવેદનશીલ ઓળખ સંબંધિત માહિતીને સોશિયલ મીડિયા પર શેર કરવાનું ટાળો અને ઍક્સેસને મર્યાદિત કરો.
- સોશિયલ મીડિયા એકાઉન્ટ્સ પર તમારા ફોટાને સાર્વજનિક રૂપે ઑનલાઇન શેર કરશો નહીં, ફક્ત મર્યાદિત માહિતી જ પોસ્ટ કરો.
- સોશિયલ મીડિયા એકાઉન્ટ પર મોકલવામાં આવેલી વિનંતીઓ પર કયારેય પૈસા મોકલશો નહીં.
- યોગ્ય પુષ્ટિ વિના અજાણ્યાઓ તરફથી મળેલી ફ્રેન્ડ રિક્વેસ્ટ ક્યારેય સ્વીકારશો નહીં.
- જ્યાં સુધી તમે સ્ત્રોતની અધિકૃતતાની ચકાસણી ન કરો ત્યાં સુધી ક્યારેય શંકાસ્પદ લિંક્સ પર ક્લિક કરશો નહીં અથવા કંઈપણ ડાઉનલોડ કરશો નહીં.
- સોશિયલ મીડિયા અને સાયબર અપરાધ વેબસાઇટ cyberciime.com.in પર કોઈપણ ફેક પ્રોફાઇલ સામે રિપોર્ટ કરો.
- સિક્યોરિટી એંડ પ્રાઇવસી સુવિધાઓથી વાકેફ રહો અને તેને સોશિયલ મીડિયા એકાઉન્ટ્સ પર ઇનેબલ કરો.

5.4 સોશિયલ એન્જિનિયરિંગ (Social Engineering)

જ્યારે સાયબર સુરક્ષાની વાત આવે છે ત્યારે મનુષ્યો સૌથી નબળી કડી છે તે ઘણીવાર પુરવાર થઈ ચૂકયું છે. ઘણા હુમલાખોરો આ નબળાઈનો લાભ લઈ તેમના સાયબર હુમલાના પ્રયાસોને સફળ બનાવવા સોશિયલ એન્જિનિયરિંગનો ઉપયોગ કરે છે. સોશિયલ એન્જિનિયરિંગ ઉપયોગી માહિતી એકત્ર કરવા માટે ટૅક્નોલૉજીને બદલે મનુષ્યોને લક્ષ્ય બનાવે છે.

સોશિયલ એન્જિનિયરિંગ શું છે ?

બેશિયલ એન્જિનિયરિંગ એ લોકોની સાથે હોશિયારીથી કે ચાલાકીથી કામ લેવાની કળા છે જેથી તેઓની ગોપનીય માહિતી જાણી શકાય. આ ગુનેગારો જે માહિતી મેળવવા પ્રયત્ન કરી રહ્યા હોય છે તેના પ્રકારો બદલાઈ શકે છે, પરંતુ જ્યારે વ્યક્તિઓને નિશાન બનાવવામાં આવે છે ત્યારે તેઓ સામાન્ય રીતે પાસવર્ડ કે બેંકની માહિતી મેળવવાનો પ્રયાસ કરતા

હોય છે. તેઓ દ્વારા કમ્પ્યૂટરમાં ગુપ્ત રીતે દૂષિત સૉફ્ટવેર ઈન્સ્ટોલ કરવા માટેનો પ્રયાસ પણ થતો હોય છે જેથી તેઓ કમ્પ્યૂટરને નિયંત્રિત કરી શકે અથવા તેમાં રહેલી માહિતીની ચોરી કરી શકે.

હુમલાખોરો સોશિયલ એન્જિનિયરિંગનો ઉપયોગ કરે છે, કારણ કે સૉફ્ટવેરને હેક કરવાની રીતો શોધવા કરતાં યુઝરની માનસિક નબળાઈઓનો ઉપયોગ કરી માહિતી કઢાવી લેવી એ સામાન્ય રીતે સરળ છે. ઉદાહરણ તરીકે, કોઈના એકાઉન્ટનો પાસવર્ડ હેક કરવાનો પ્રયાસ કરવા કરતાં કોઈ વ્યક્તિને તેનો પાસવર્ડ આપવા માટે મૂર્ખ બનાવવું તે કદાચ વધુ સરળ છે.

સોશિયલ એન્જિનિયરિંગ માટે હુમલાખોરો ફોન કોલ્સ, ઈ-મેઈલ અથવા ટેક્સ્ટ મેસેજનો ઉપયોગ કરી શકે છે. ઘણીવાર તેઓ ટેક સપોર્ટ અથવા બેંક કર્મચારીઓ તરીકે પોતાની ખોટી ઓળખ આપે છે અને લક્ષ્ય પાસેથી માહિતી એકઠી કરે છે. આમ કરનારાઓને કેટલીકવાર 'માનવ હેકર્સ' તરીકે પણ ઓળખવામાં આવે છે.

સોશિયલ એન્જિનિયરિંગ કેવી રીતે કામ કરે છે ?

મોટાભાગના સોશિયલ એન્જિનિયરિંગ હુમલા, હુમલાખોરો અને પીડિતો વચ્ચેના વાસ્તવિક સંચાર પર આધાર રાખે છે. સોશિયલ એન્જિનિયરિંગમાં નીચે મુજબના તબક્કાઓ સામેલ છે.

- **રિકોનિસન્સ :** આ તબક્કા દરમ્યાન હુમલાખોર લક્ષ્ય વિશેની માહિતી એકત્ર કરે છે, જેમ કે તેમની રુચિઓ, ટેવો અને સામાજિક જોડાણો.
- **લક્ષ્યની પસંદગી :** હુમલાખોર રિકોનિસન્સ તબક્કા દરમિયાન એકત્ર કરવામાં આવેલી માહિતીના આધારે ચોક્કસ લક્ષ્ય પસંદ કરે છે.
- **લક્ષ્ય સાથે સંબંધ પ્રસ્થાપિત કરવો :** હુમલાખોર ઘણીવાર મૈત્રીપૂર્ણ વાતચીત દ્વારા અથવા સામાન્ય હિતોની વહેંચણી દ્વારા વિશ્વાસ બનાવીને લક્ષ્ય સાથે સંબંધ સ્થાપિત કરે છે.
- **કેળવેલા સંબંધનો દુરુપયોગ કરવો :** એકવાર લક્ષ્ય સાથે વિશ્વાસ સ્થાપિત થઈ જાય પછી, હુમલાખોર લક્ષ્ય સાથે ઈચ્છિત ક્રિયા કરવા માટે ચાલાકી કરવાનું શરૂ કરે છે, જેમ કે તેની પાસેથી સંવેદનશીલ માહિતી જાહેર કરાવવી અથવા પ્રતિબંધિત વિસ્તારો કે વિવિધ સોશિયલ મીડિયા એકાઉન્ટ્સ તથા બેંક એકાઉન્ટની ઍક્સેસ આપવી.
- **હુમલો કરવો :** હુમલાખોરે એકવાર લક્ષ્યના એકાઉન્ટનો ઍક્સેસ પ્રાપ્ત કરી લીધો એટલે તે પોતાના નક્કી કરેલા ધ્યેયને હાંસલ કરવા માટે હુમલો કરે છે.
- **પુરાવાઓનો નાશ કરવો :** હુમલાખોર તેમને કરેલ હુમલાનાં પુરાવાઓને નાશ કરવા માટે તેમને લક્ષ્યને મોકલેલા ઈ-મેઈલ, સંદેશાઓનો નાશ કરવો, બ્રાઉઝિંગ ઇતિહાસ સાફ કરવી વગેરે જેવી ક્રિયાઓ કરે છે.

આ પ્રક્રિયા એક જ ઈ-મેઈલમાં અથવા સોશિયલ મીડિયા ચેટ્સની શ્રેણીમાં મહિનાઓ સુધી થઈ શકે છે. તે સામ-સામે વાતચીત પણ હોઈ શકે છે પરંતુ એ નોંધવું અગત્યનું છે કે તમામ સોશિયલ એન્જિનિયરિંગ હુમલાઓ ઉપર જણાવેલા ચોક્કસ ક્રમને અનુસરતા નથી, અને કેટલાક હુમલાખોરો ચોક્કસ પરિસ્થિતિના આધારે ચોક્કસ પગલાંને છોડી પણ શકે છે અથવા પુનરાવર્તન પણ કરી શકે છે.

સોશિયલ એન્જિનિયરિંગના પ્રકાર

સોશિયલ એન્જિનિયરિંગને બે સામાન્ય પ્રકારોમાં વિભાજિત કરી શકાય છે જેમાં પ્રથમ છે માનવ આધારિત સોશિયલ એન્જિનિયરિંગ અને બીજો છે કમ્પ્યૂટર આધારિત સોશિયલ એન્જિનિયરિંગ.

1. **માનવ આધારિત :** માનવ આધારિત સોશિયલ એન્જિનિયરિંગને માનવીઓ સાથે ક્રિયા-પ્રતિક્રિયાની જરૂર છે. તેનો અર્થ વ્યક્તિ-થી-વ્યક્તિનો સંપર્ક થયા પછી ઇચ્છિત માહિતી પ્રાપ્ત કરવી એવો થાય છે. લોકો માનવ આધારિત સોશિયલ એન્જિનિયરિંગની તકનીકોનો અલગ અલગ રીતે ઉપયોગ કરે છે.

2. **સ્વાંગ રચવો :** આ પ્રકારના સોશિયલ એન્જિનિયરિંગ હુમલામાં, હેકર પોતે કર્મચારી અથવા માન્ય વપરાશકર્તા હોવાનો ઢોંગ કરે છે.

3. **મહત્ત્વપૂર્ણ વપરાશકર્તા તરીકે વર્તવું :** આ પ્રકારના હુમલામાં, હેકર પોતે VIP અથવા ઉચ્ચ-સ્તરના મેનેજર હોવાનો ઢોંગ કરે છે, જેની પાસે કમ્પ્યૂટર સિસ્ટમ અથવા ફાઈલોનો ઉપયોગ કરવાની સત્તા છે. મોટેભાગે, નિમ્ન-સ્તરના કર્મચારીઓ આવા પદ પર રહેલા વ્યક્તિને કોઈ પ્રશ્ન પૂછતા નથી જેથી હેકર ખૂબ સરળતાથી હુમલો કરી શકે છે.

- **ત્રીજી વ્યક્તિ તરીકે વર્તવું :** આ હુમલામાં હેકર કોમ્પ્યૂટર સિસ્ટમનો ઉપયોગ કરવા માટે અધિકૃત વ્યક્તિ પાસેથી પરવાનગી લીધેલ હોવાનો ડોળ કરે છે. જ્યારે અધિકૃત વ્યક્તિ અમુક સમય માટે ઉપલબ્ધ ન હોય ત્યારે તેઓ આ કાર્ય કરે છે.

2. **કમ્પ્યૂટર આધારિત :** કોમ્પ્યૂટર આધારિત સોશિયલ એન્જિનિયરિંગ, કમ્પ્યૂટર સોફ્ટવેરનો ઉપયોગ કરે છે જે ઇચ્છિત માહિતી પ્રાપ્ત કરવાનો પ્રયાસ કરે છે.

- **ફિશિંગ :** આ શબ્દ કાયદેસરના વ્યવસાય, બેંક અથવા ક્રેડિટ કાર્ડ કંપની તરફથી માહિતીની ચકાસણી માટે વિનંતી કરતો અને જો તે કરવામાં ન આવે તો કેટલાક ભયંકર પરિણામોની ચેતવણી આપતા ઈ-મેઈલ કે સંદેશા માટે લાગુ પડે છે. આવા ઈ-મેઈલ કે સંદેશમાં નકલી વેબ પેજની લિંક હોય છે જે વાસ્તવિક વેબ પેજ જેવું જ દેખાય છે અને તેમાં રહેલ ફોર્મ વપરાશકર્તાનાં નામ, પાસવર્ડ, કાર્ડ નંબર અથવા પિન વગેરેની વિગતો આપવા વિનંતી કરી શકે છે.
- **વિશિંગ :** આ નાણાકીય પુરસ્કારના હેતુથી જાહેર જનતા પાસેથી ખાનગી અને નાણાકીય માહિતી મેળવવા માટે વોઈસ ઓવર ઈન્ટરનેટ પ્રોટોકોલ (VoIP) ટેક્નોલૉજીનો લાભ લેવાની રીત છે.
- **પોપઅપ વિન્ડો :** આમાં હુમલાખોરનો માલવેર (નુકસાનકર્તા પ્રોગ્રામ) પોપઅપ વિન્ડો જનરેટ કરે છે, જે કહે છે કે નેટવર્ક સમસ્યાઓને કારણે એપ્લિકેશન કનેકિટવિટી બંધ થઈ ગઈ હતી અને હવે વપરાશકર્તાએ તેનું સત્ર ચાલુ રાખવા માટે તેનું આઈડી અને પાસવર્ડ ફરીથી દાખલ કરવાની જરૂર છે.
- **રસપ્રદ સૉફ્ટવેર :** આ કિસ્સામાં પીડિતને ખૂબ જ ઉપયોગી પ્રોગ્રામ અથવા એપ્લિકેશન ડાઉનલોડ અને ઇન્સ્ટોલ કરવા માટે સહમત કરવામાં આવે છે જે CPU પ્રદર્શન વધારનાર અથવા તો સિસ્ટમની ઉપયોગિતા વધારનાર સોફ્ટવેરના સ્વરૂપે 'સ્પાયવેર' અથવા 'માલવેર' હોઈ શકે છે. ઉદાહરણ તરીકે કી લોગર (Key Logger) જે એકવાર ઇન્સ્ટોલ થઇ ગયા પછી જે તે સિસ્ટમમાં જેટલી પણ કી પ્રેસ થાય છે તેની માહિતી ચોક્કસ વ્યક્તિને પહોંચાડે છે.

સોશિયલ એન્જિનિયરિંગ દ્વારા વ્યક્તિની લાલચનો લાભ લઈ માહિતી મેળવવા માટે કરવામાં આવતા ઈ-મેઈલનું ઉદાહરણ

સોશિયલ એન્જિનિયરિંગ સામે રક્ષણ

સોશિયલ એન્જિનિયરિંગ પ્રકારના હુમલાઓ સામે રક્ષણ મેળવવા માટે નીચે મુજબના મુદ્દાઓનું અનુસરણ કરવું.

- કોઈપણ શંકાસ્પદ કોલ્સ, ઈ-મેઈલ અથવા ટેક્સ્ટની ચકાસણી અચૂક કરો.
- ફક્ત વિશ્વસનીય સ્ત્રોતોમાંથી આવેલા જોડાણો જ ખોલો.
- પાસવર્ડ અથવા પોતાને લગતી સંવેદનશીલ માહિતી, જેમ કે ક્રેડિટ કાર્ડ નંબર અથવા નાણાકીય માહિતી માટે પૂછતા કોઈપણ ઇ-મેઇલ અથવા ટેક્સ્ટને તરત જ કાઢી નાખો.
- ઈનામોનું વચન આપતા કોઈપણ લોભામણા ઈ-મેઈલને ખોલશો નહીં.
- કોઈપણ સોફ્ટવેર ડાઉનલોડ કરવા માટે માત્ર માન્ય સ્ત્રોતોમાંથી કરો.
- કોઈ વ્યક્તિની કોઈપણ માધ્યમ દ્વારા તાત્કાલિક નાણાકીય મદદ માટેની વિનંતીઓથી સાવચેત રહો.
- તમારી પાસે તમારા ઉપકરણ પર સ્પામ ફિલ્ટર્સ અને એન્ટિવાયરસ સોફ્ટવેર ઈન્સ્ટોલ કરો.

સોશિયલ એન્જિનિયરિંગ હુમલાના કેટલાક પ્રખ્યાત કિસ્સાઓ :

- **ટ્વિટર બિટકોઈન કૌભાંડ - 2020 (Twitter Bitcoin Scam - 2020) :** ટ્વિટર બિટકોઈન કૌભાંડ તાજેતરના સાયબર હુમલાઓમાંનું એક હતું, જે દર્શાવે છે કે સોશિયલ મીડિયા જાયન્ટ્સ પણ સાયબર હુમલાઓ પ્રત્યે સંવેદનશીલ હોઈ શકે છે. વિશ્વસનીય બ્લુ વેરિફિકેશન ચેકમાર્ક સાથેના જાણીતા ટ્વિટર યુઝર્સે 'તમારા બિટકોઇનને બમણું કરો' ઑફર ટ્વીટ કરી, તેમના ફોલોવરર્સને જાણ કરી કે ચોક્કસ લિંક દ્વારા કરવામાં આવેલ દાન બમણું થઇ જશે. ધ બીબીસીના જણાવ્યા મુજબ, લક્ષ્યાંકિત એકાઉન્ટ્સના લાખો ફોલોવર હોવાના કારણે, હેકરોએ મિનિટોમાં સેંકડો યોગદાન મેળવ્યા હતા, જે બિટકોઈનમાં કુલ **$** 100,000 કરતાં વધુ હોવાનું કહેવાય છે.
- **ટોયોટા (2019) :** 2019 માં, ઓટો પાર્ટ્સ સપ્લાયર ટોયોટા બોશોકુ કોર્પોરેશનને સોશિયલ એન્જિનિયરિંગ અને BEC (બિઝનેસ ઈ-મેઈલ કોમ્પ્રોમાઈઝ) હુમલાએ નિશાન બનાવ્યો હતો. વધુમાં, હુમલાખોરોએ ફાઈનાન્સ એક્ઝિક્યુટિવને વાયર ટ્રાન્સફરમાં પ્રાપ્તકર્તાના બેંક એકાઉન્ટની માહિતી અપડેટ કરવા માટે સમજાવ્યા.
- **યાહૂ હેક (2014) :** 2014 યાહૂ હુમલામાં કર્મચારીઓને લક્ષ્યાંક બનાવતા સ્પિયરફિશિંગ હુમલાનો ઉપયોગ કરવામાં આવ્યો હતો. એક કર્મચારી ઈ-મેલ થકી ભ્રમિત થઈને, હુમલાખોરને Yahoo નેટવર્કની ઍક્સેસ આપી અને તેમને Yahoo વપરાશકર્તા ડેટાબેઝ ડાઉનલોડ કરવાની મંજૂરી આપી. રિકવરી ઇ-મેઇલ સરનામાંનો ઉપયોગ કરીને, હેકર્સે કામના એકાઉન્ટને ઓળખ્યા અને નકલી યાહૂ કૂકીઝ બનાવવા માટે ડેટાબેઝમાં સંગ્રહિત ક્રિપ્ટોગ્રાફિક મૂલ્યોનો ઉપયોગ કર્યો. આનાથી તેમને 6,500 યાહૂ યુઝર એકાઉન્ટ્સ સાથે સંપૂર્ણપણે ચેડા કરીને પાસવર્ડ વિના વપરાશકર્તાના એકાઉન્ટને ઍક્સેસ કરવાની મંજૂરી મળી.

5.5 ફેક ન્યુઝ / નકલી સમાચારો (Fake News)

નકલી સમાચાર શું છે ?

ક્યારેક તમે મોબાઈલ અથવા તમારા કમ્પ્યૂટરની સ્ક્રીન ઉપર અણધાર્યા સમાચાર જોયા હશે કે જે ખોટી કે ભ્રામક માહિતી લોકો સુધી પહોચાડવા પ્રકાશિત કરવામાં આવે છે. કોઈ પ્રતિષ્ઠિત વ્યક્તિનાં જીવન અંગે ખોટી વાત ફેલાવવી, દેશમાં કે વિદેશમાં ચર્ચાઈ રહેલા કોઈ મુદ્દાને અનુલક્ષીને ખોટી વાત ફેલાવવી, લોકોને જેમાં વધુ રસ હોય તેવી વાતને અનુરૂપ કોઈ ખોટો સંદેશો પ્રકાશિત કરવો વગેરે નકલી સમાચારોના કેટલાક ઉદાહરણો છે.

ખોટા સમાચારો ફેલાવવા એ કોઈ નવી ઘટના નથી, વાસ્તવમાં 19મી સદીમાં 'ફેક ન્યૂઝ' શબ્દનો ઉપયોગ કરવામાં આવ્યો હતો પરંતુ તે સમયે નકલી સમાચારોનો વ્યાપ આજના જેટલો ન હતો. આજના સમયમાં ઈન્ટરનેટ અને સોશિયલ મીડિયાને કારણે 'ફેક ન્યૂઝ' સમાજના મોટાભાગના લોકો સુધી ખૂબ જ ઓછા સમયમાં પહોંચી જાય છે અને એટલે જ તેની અસરકારકતા પણ વધી છે. ઈન્ટરનેટનો વ્યાપ ઓછો હતો ત્યારે લોકો વિશ્વસનીય મીડિયા સ્ત્રોતો પાસેથી જ સમાચાર પ્રાપ્ત કરવાનું વલણ ધરાવતા હતા કે જેમના પત્રકારોએ પત્રકારિતાના કડક નિયમોનું પાલન કરવું જરૂરી હતું અને એટલે જ પ્રમાણભૂત સમાચારોનું પ્રવર્તન થતું હતું પરંતુ અત્યારે તો ઈન્ટરનેટે પ્રમાણમાં ઓછા નિયમન અથવા સંપાદકીય ધોરણો સાથે સમાચાર અને માહિતીને પ્રકાશિત કરવા, શેર કરવા અને વપરાશ કરવાની નવી રીતો લોકો સમક્ષ આપી છે. ઘણા લોકો હવે સોશિયલ મીડિયા અને અન્ય ઓનલાઈન સ્ત્રોતોમાંથી સમાચારો જાણવાનું વધુ પસંદ કરે છે પરંતુ સમાચારો વિશ્વસનીય છે કે નહિ તે ચકાસવાની દરકાર ઘણીવાર રાખતા નથી.

નકલી સમાચારના પ્રકાર :

નકલી સમાચારના વિવિધ પ્રકારો છે, જે તેને બનાવનારાઓની ખોટા સમાચારો બનાવવાની પ્રેરણા પર આધાર રાખે છે.

- **ક્લિકબાઈટ :** ક્લિકબાઈટ પ્રકારના ખોટા સમાચારોનો ઉપયોગ ઈરાદાપૂર્વક વેબસાઇટના મુલાકાતીઓની સંખ્યા વધારવા માટે થાય છે જેના દ્વારા વેબસાઇટનાં માલિકો વેબસાઈટમાં મૂકવામાં આવેલ જાહેરાતની આવકમાં વધારો કરી શકે છે.
- **પ્રચાર કરવા માટે :** ઘણી વખત વ્યક્તિઓને ગેરમાર્ગે દોરવા અથવા રાજકીય એજન્ડા અથવા પક્ષપાતી પરિપ્રેક્ષ્યને પ્રોત્સાહન આપવા માટે ખોટી અથવા અચોક્કસ વાતોને પ્રકાશિત કરવામાં આવે છે.
- **નબળી ગુણવત્તાયુક્ત પત્રકારત્વ :** કેટલીકવાર, પત્રકારો પાસે પ્રકાશિત કરતા પહેલા જે સમાચાર તેઓ પ્રકાશિત કરી રહ્યા છે તેમની તમામ હકીકતો તપાસવાનો સમય હોતો નથી, જેના કારણે તેમેની સાચી ભૂલો નકલી સમાચાર બની જાય છે.
- **ભ્રામક હેડલાઈન્સ :** કેટલીકવાર સમાચાર વ્યાપક રીતે સાચા હોઈ શકે છે, પરંતુ તેના પર ક્લિક કરવા માટે વાચકોને લલચાવવા માટે સનસનાટીભર્યા અથવા ભ્રામક હેડલાઈનનો ઉપયોગ કરવામાં આવે છે જે બાદમાં નકલી સમાચાર તરફ દોરી શકે છે.
- **ઈમ્પોસ્ટર સામગ્રી :** આમાં ઘણી વખત પ્રેક્ષકોને છેતરવા અથવા ગેરમાર્ગે દોરવા માટે સાચા સમાચાર સ્ત્રોતોને ખોટી, બનાવેલી વાતો સાથે જોડી દેવામાં આવે છે.

પ્રખ્યાત નકલી સમાચાર ઉદાહરણો :

- **કોરોનાવાયરસ અંગેનાં નકલી સમાચાર :** સાલ 2020-2021 માં કોવિડ19

રોગચાળાનો વ્યાપ જ્યારે ખૂબ જ હતો ત્યારે આ વાયરસ સંબંધિત ઘણાબધાં ખોટા સમાચારો ફરતા થયેલા જેમ કે એક દાવો એવો હતો કે "5G ટૅક્નોલૉજી વાયરસના ફેલાવા સાથે જોડાયેલી છે કારણ કે 5G રોગપ્રતિકારક શકિતને દબાવી દે છે જ્યારે વાયરસ રેડિયો તરંગો દ્વારા સંચાર કરે છે." આ દાવાઓ સાચા નહોતા અને અધિકૃત સ્ત્રોતો દ્વારા તેને વારંવાર નકારી કાઢવામાં આવ્યા હતા પરંતુ તેમ છતાં આ પ્રકારના ખોટા સમાચારો વ્યાપકપણે શેર કરવામાં આવ્યા હતા.

- **2016માં યુએસ પ્રમુખપદની ચૂંટણી :** 2016 માં US માં પ્રમુખપદની ચૂંટણી દરમિયાન સમગ્ર રાજકીય સ્પેક્ટ્રમમાં ખોટા અને ભ્રામક દાવાઓ સાથે નકલી સમાચાર અને ખોટી માહિતી પ્રસ્તુત કરવામાં આવી હતી જે એક મોટો મુદ્દો બની ગયો હતો. એક વિશ્લેષણ સૂચવે છે કે ચૂંટણીમાં બનાવવામાં આવેલા બનાવટી સમાચારોનો મોટો હિસ્સો મેસેડોનિયાના કિશોરો દ્વારા બનાવવામાં આવ્યો હતો, જેનો હેતુ વધુમાં વધુ લોકો આવા ખોટા સમાચારો ઉપર ક્લિક કરે અને તેને શેર કરે અને પરિણામે ખોટી માહિતી મૂકનારી વ્યક્તિ વધુમાં વધુ પૈસા કમાય શકે.

0 **નવી નોંધોમાં કિરણોત્સર્ગી શાહી છે :** જ્યારે 2016ની સાલમાં ભારતમાં નોટબંધી કરવામાં આવી અને ત્યાર બાદ નવી ચલણી નોટો પ્રસિદ્ધ કરવામાં આવી ત્યારે એક એવા સમાચાર પ્રસારીત થયેલા કે "RBI રૂ. 2,000 અને રૂ. 500ની નવી નોટો છાપવા માટે કિરણોત્સર્ગી શાહીનો ઉપયોગ કરી રહી છે. નવી નોટોમાં 'ફોસ્ફરસ (P32)ના કિરણોત્સર્ગી આઈસોટોપનો સમાવેશ થાય છે" નકલી સમાચારમાં એવો પણ દાવો કરવામાં આવ્યો હતો કે 'આવકવેરા વિભાગ ચોક્કસ સ્થળે રોકડના મોટા જથ્થાને શોધી કાઢવા માટે આઈસોટોપનો ઉપયોગ કરી રહ્યું છે. આની સાથે સાથે એવા સમાચારો પણ પ્રસારીત કરવામાં આવેલા કે આ ચલણી નોટોમાં ઈલેક્ટ્રોનિક ચીપ પણ મૂકવામાં આવી છે જેના દ્વારા ચલણી નોટોની ખરાઈ કરી શકાય.'

નકલી સમાચાર કેવી રીતે ફેલાય છે ?

- નકલી સમાચાર ઘણીવાર કેટલીક વેબસાઈટ દ્વારા ફેલાવવામાં આવે છે, જેમાં આ સમાચારો ખૂબ જ આકર્ષક રીતે રજૂ કરવામાં આવે છે જેથી લોકો તે વાંચવા માટે આકર્ષાય.
- સોશિયલ મીડિયા પણ ખોટા સમાચારોને ઝડપથી ફેલાવવા માટે સક્ષમ કરે છે. સોશિયલ મીડિયા ફીડ્સ ઘણીવાર રીલેશનશીપ મેટ્રિક્સના આધારે સામગ્રીને પ્રાથમિકતા આપે છે એટલે કે, તે કેટલી વાર શેર કરવામાં આવે છે અને તેને કેટલા લોકો દ્વારા પસંદ કરવામાં આવે છે વગેરે જેવા પરિબળોને આધારે પણ ખોટા સમાચારો સોશિયલ મીડિયામાં ફેલાય છે.
- સોશિયલ મીડિયા બૉટ્સ નકલી સમાચાર ફેલાવી શકે છે કારણ કે તેઓ તેમના સ્ત્રોતોની વિશ્વસનીયતાને ધ્યાનમાં લીધા વિના મોટા પ્રમાણમાં લેખોનું ઉત્પાદન કરે છે અને ફેલાવે છે. બોટ્સ ઑનલાઈન નકલી એકાઉન્ટ પણ બનાવી શકે છે, જેનો ઉપયોગ ખોટી માહિતીનાં બહોળા પ્રચાર માટે થાય છે.
- કેટલાક ઈન્ટરનેટ વપરાશકર્તાઓ પૈસા મેળવવા માટે પણ ખોટી માહિતી કે સમાચારોને ફેલાવતા હોય છે.
- વિવિધ સોફ્ટવેર, મશીન લર્નિંગ અને ફેસ-સ્વેર્પિંગ ઉપયોગ કરીને ઘણીવાર નકલી વીડિયો બનાવવામાં આવે છે અને તેમાં એવી ઘટના બતાવવામાં આવે છે કે જે

ઘટનાઓ અથવા ક્રિયાઓ વાસ્તવમાં ક્યારેય થઈ નથી. વિવિધ વેબસાઈટ અને સોશિયલ મીડિયાનાં માધ્યમ દ્વારા આવા નકલી વિડીયો લોકો સુધી પહોચાડી વ્યક્તિ અથવા વસ્તુની પ્રતિષ્ઠાને હાનિ પહોચાડવામાં આવે છે.

નકલી સમાચાર કેવી રીતે ઓળખવા ?

નીચે ખોટી માહિતી ઓળખવા, નકલી સમાચાર વેબસાઇટ્સ ઓળખવા અને શેર કરતા પહેલા વિચારવા માટેની કેટલીક યુક્તિઓ છે :

- **વેબસાઈટની URL તપાસો :** તમે જે વેબસાઈટ જોઈ રહ્યાં છો તેની URL ચકાશો. મોટાભાગે કોઈ જાણીતી વેબસાઈટની URLમાં એકાદ અક્ષરનો ફેર કરી ડમી URL બનાવવામાં આવે છે જેથી વેબસાઈટ વાપરનાર લોકોને ભરમાવી શકાય. તેથી તમે જે વેબસાઈટ જોઈ રહ્યા છો તેની URLની ખરાઈ અચૂક કરવી.
- **લેખકને તપાસો :** જે લેખ આપ વાંચી રહ્યા છો તેના લેખકને તપાસો. તેની વિશ્વસનીયતાની ખરાઈ અચૂક કરો. શું લેખક આપ જે વાંચી રહ્યા છો તે વિષયમાં જાણકાર છે કે કેમ તે તપાસી જોવું. જો લેખમાં લખાયેલ વિવરણ અજુગતું લાગે તો આ લખવા પાછળ લેખકની પ્રેરણા શું હોઈ શકે તે પણ ધ્યાનમાં લો.
- **અન્ય સ્ત્રોતો તપાસો :** આપ જે સમાચારો વાંચી રહ્યા છો તેમાં આપને કંઈક અયોગ્ય લાગે તો અન્ય પ્રતિષ્ઠિત સમાચાર અથવા મીડિયા આઉટલેટ્સનાં સ્ત્રોત પણ ચકાશો જેથી સમાચારોની ખરી થઇ શકે.
- **નિર્ણાયક માનસિકતા જાળવી રાખો :** ડર અથવા ગુસ્સો જેવી મજબૂત ભાવનાત્મક પ્રતિક્રિયાઓ ઉશ્કેરવા માટે ઘણાં નકલી સમાચારો હોશિયારીથી લખવામાં આવે છે. આવા સમાચારોથી પ્રભાવિત થતા પહેલા તમારી જાતને પૂછો કે આ સમાચાર શા માટે લખવામાં આવ્યા છે ? શું તે કોઈ ચોક્કસ કારણ અથવા એજન્ડાને પ્રોત્સાહન આપી રહ્યું છે ? શું તે મને બીજી વેબસાઇટ પર ક્લિક કરવા માટે પ્રયાસ કરી રહ્યો છે ? આવી રીતે વિવેકથી વિચારી પ્રતિક્રિયા આપો.
- **હકીકતો તપાસો :** વિશ્વસનીય સમાચાર વાર્તાઓમાં પુષ્કળ તથ્યોનો સમાવેશ થશે- ડેટા, આંકડા, નિષ્ણાતોના અવતરણો વગેરે. જો આ ખૂટે છે, તો આપ જે સમાચાર વાંચી રહ્યા છો તેને બીજા કોઈ સ્ત્રોત દ્વારા ચકાશો.
- **ટિપ્પણીઓ તપાસો :** ઘણીવાર લેખ અથવા વિડિયો કાયદેસર હોવા છે પરંતુ તેની નીચેની ટિપ્પણીઓ બોટ્સ દ્વારા અથવા ગેરમાર્ગે દોરતી અથવા ગૂંચવણભરી માહિતી મૂકવા માટે ભાડે રાખેલા લોકો દ્વારા તૈયાર થયેલ હોય શકે છે. તેથી તે ટિપ્પણીઓ ઉપર વિશ્વાસ કરતા પહેલા તેને યોગ્ય રીતે ચકાશો.

5.6 રૂપરેખા સમાધાન (Profile Compromised)

આજનો યુગ ટેક્નોલૉજીનો યુગ છે અને આ સમયમાં ઈન્ટરનેટની પ્રાપ્યતા તથા મોબાઈલના વધતા જતા ઉપયોગને કારણે ઓનલાઈન સોશિયલ નેટવર્ક્સ, જેમ કે ફેસબુક, ટ્વિટર, ઈન્સ્ટાગ્રામ, વગેરે લોકો માટે વિશ્વ સાથે સંપર્કમાં રહેવા માટેનું એક મુખ્ય માધ્યમ બની ગયા છે. સેલિબ્રિટીઓ તેમના ચાહકો સાથે વાતચીત કરવા માટે, વિવિધ કંપનીઓ તેમની બ્રાન્ડને પ્રમોટ કરવા અને તેમના ગ્રાહકો સાથે સીધો સંપર્ક કરવા, સમાચાર એજન્સીઓ બ્રેકિંગ ન્યૂઝને વહેલામાં વહેલી તકે લોકો સુધી પહોંચાડવા માટે સોશિયલ નેટવર્કનો લાભ લે છે. વિશ્વના ઘણા બધાં લોકો તેમના મિત્રો સાથે સંપર્કમાં રહેવા અને વિવિધ ઉપયોગી અને રસપ્રદ લાગે તેવી માહિતી મિત્રોને મોકલવા સોશિયલ નેટવર્ક્સનો

 ઉપયોગ વ્યાપક પ્રમાણમાં કરે છે.

સોશિયલ મીડિયા વપરાશકર્તાઓ સોશિયલ નેટવર્ક્સમાં જેને અનુસરે (Follow) કરે છે તેની સાથે વિશ્વાસનો નાતો બનાવે છે એટલે કે જેને તે અનુસરે (Follow કરે) છે તેના દ્વાર સોશિયલ મીડિયામાં જે પણ માહિતી મૂકવામાં આવે છે તેને વપરાશકર્તા તરત જ સ્વીકારી લે છે. કમનસીબે, જો આવા કોઈ સોશિયલ મીડિયા એકાઉન્ટનું નિયંત્રણ સાયબર ગુનેગાર (Cyber Criminal)ના હાથમાં આવી જાય, તો તે પોતાના અયોગ્ય કાર્યોને આગળ વધારવા માટે આ વિશ્વાસનો સરળતાથી ઉપયોગ કરી શકે છે. એક સંશોધનો પ્રમાણે દૂષિત વિષયવસ્તુ (Malicious Content) ફેલાવવા માટે ચેડાં (Hack) કરેલા એકાઉન્ટ્સનો ઉપયોગ સાયબર ગુનેગારો (Cyber Criminal) માટે ફાયદાકારક છે, કારણ કે સોશિયલ નેટવર્ક વપરાશકર્તાઓ તેમના વિશ્વાસ કરતા એકાઉન્ટ્સમાંથી આવતા સંદેશાઓ પર તરત પ્રતિક્રિયા આપે છે.

પ્રોફાઈલ સમાધાન (Profile Compromised) શું છે ?

આવો પ્રોફાઇલ સમાધાન (Profile Compromised) ને એક ઉદાહરણથી સમજીએ. Mr. X ફેસબુકનો ઉપયોગ કરે છે અને ઘણા બધા ફોલોઅર્સ ધરાવે છે. Mr. Y ને Mr. X એ સોશિયલ નેટવકર્સમાં પ્રાપ્ત કરેલ લોકપ્રિયતાની ઈર્ષા આવે છે અને તે ગમે તેમ કરી Mr. X નાં ફોલોઅર્સની સંખ્યા ઘટાડવા માંગે છે. આ માટે તેણે તેને છેતરવાનું નક્કી કર્યું. Mr. Y એ Mr. X ને કોઈ એક ઈ-મેઈલ અથવા લીંક મોકલી જેમાં તેને જણાવ્યું કે Mr. X નાં ફેસબુક એકાઉન્ટની સુરક્ષા વધારવાની છે જેના માટે તેનો ફેસબુક પાસવર્ડ માંગ્યો. Mr. X એ આવા મેસેજ કે લીંકથી ભરમાઈ જઈ પોતાનો પાસવર્ડ Mr. Y ને મોકલ્યો. Mr. Y એ આનો લાભ લીધો અને Mr. Xનાં એકાઉન્ટમાં લોગ ઇન કર્યું. ત્યારપછી તેણે તરત જ પાસવર્ડ બદલી નાખ્યો અને Mr. Xના તમામ અનુયાયીઓ (Followers) ને Mr. Xના એકાઉન્ટમાંથી અયોગ્ય કે દૂષિત સંદેશા મોકલવાનું શરૂ કર્યું. આના કારણે ઘણા લોકોએ Mr. X ને અનુસરવાનું બંધ કર્યું અને તેની લોકપ્રિયતામાં પણ ખૂબ જ ઘટાડો થયો. આવી રીતે Mr. Y એ Mr. X ની પ્રોફાઇલ સમાધાન (Compromised) કરી પોતાનું કાર્ય પૂર્ણ કર્યું.

જ્યારે દૂષિત વિષયવસ્તુ (Malicious Content) ફેલાવવા માટે અથવા અયોગ્ય કાર્યોને અંજામ આપવા કાયદેસર (Legal) સોશિયલ મીડિયા એકાઉન્ટ્સ હેક કરવામાં આવે ત્યારે પ્રોફાઇલ સમાધાન (Compromised) થાય છે. જ્યારે કોઈ તમારું એકાઉન્ટ ‘હેક’ કરે છે, ત્યારે તેઓ ખરેખર એકાઉન્ટ પર નિયંત્રણ મેળવે છે. હેકર્સ પાસવર્ડનું અનુમાન લગાવી, ફિશિંગ (ભ્રામક) ઈ-મેઈલમાં દૂષિત લિંક દ્વારા અથવા દૂષિત (Malicious) એપ્લિકેશન ઇન્સ્ટોલ કરાવીને એકાઉન્ટમાં પ્રવેશ મેળવે છે અને તેનો ફાવે તેમ ઉપયોગ કરી શકે છે. ઘણા બધા હેકર આવી રીતે બીજા કોઈની પ્રોફાઇલ સમાધાન (Compromised) કરી જે તે વ્યક્તિના હેક થયેલ એકાઉન્ટ સાથે જોડાયેલા લોકોને ખોટા સંદેશા મોકલી શકે, તેમના કમ્પ્યુટરને હેક કરવા માટે દૂષિત (Malicious) લીંક મોકલી શકે, બીજા હેકર્સને મિત્ર બનાવવા માટે વિનંતી (Friend Request) મોકલી શકે. આ દરેક પરિસ્થિતિમાં જે વ્યક્તિને આવા ખોટા સંદેશ અથવા લીંક પ્રાપ્ત થાય છે તેમની નજરમાં તમે જ ગુનેગાર ઠરો છો કારણ કે આ બધી જ ક્રિયા તમારા એકાઉન્ટમાંથી થયેલ છે.

સમાધાન થયેલ પ્રોફાઈલ દ્વારા પૈસાની માંગણી

શા માટે હેકર્સ સોશિયલ મીડિયા પ્રોફાઇલ સમાધાન (Profile Compromised) કરે છે ?

સાયબર ગુનેગાર (Cyber Criminal)નીચે જણાવેલ કારણોને લીધે કોઈની પ્રોફાઇલ સમાધાન (Compromised) કરે છે.

- **આનંદ માટે :** કેટલીકવાર હેકર્સ કોઈના એકાઉન્ટ પર નિયંત્રણ લઈ લે છે અને કંઈક એવું પોસ્ટ કરે છે જે તેમને રમુજી લાગે છે. આ પ્રકારના પ્રોફાઈલ કોમ્પ્રોમાઈઝથી વ્યક્તિની ગોપનીયતાનો ભંગ થાય છે પરંતુ આ સિવાય છે. કોઈ મોટું નુકસાન થતું નથી.
- **બળજબરીપૂર્વક સંદેશા મોકલવા માટે :** સોશિયલ મીડિયા એકાઉન્ટ હેક થવાનું બીજું કારણ અયોગ્ય સંદેશાઓને બળજબરીપૂર્વક લોકો સુધી મોકલવાનું છે. ઉદાહરણ તરીકે, Mr. Y પોતાના વ્યવસાયને પ્રોત્સાહન આપવા માટે Mr. Xના વિશાળ અનુયાયીઓ (Followers)નો લાભ લેવા માંગતો હોય અને તેથી તેણે Mr. Xની પ્રોફાઇલ કોમ્પ્રોમાઈઝ કરી અને તેના તમામ અનુયાયીઓ (Followers)ને પોતાના વ્યવસાયને લગતા સંદેશાઓ મોકલી તેની મુલાકાત લેવા અને વધુ શેર કરવાનું કહી શકે છે. આ ઉપરાંત કોઈ હેકર પોતાના દૂષિત ઈરાદોઓને પૂર્ણ કરવા માટે ટ્રોજન હોર્સ, ફિશિંગ વેબ પેજ અને વિવિધ પ્રકારના માલવેરની લીંક આકર્ષક લાગે તેવી રીતે મોકલી મોટું નુકસાન કરી શકે છે.
- **ગેરકાયદેસર પ્રોફાઈલને બળજબરીપૂર્વક અનુસરવા માટે :** કોઈ એક ગેરકાયદેસર પ્રોફાઈલને અનુસરવા (Follow) માટે એક વ્યાપક યોજનાના ભાગ રૂપે કોઈ સોશિયલ મીડિયા એકાઉન્ટને હેક કરવામાં આવી શકે છે. ગેરકાયદેસર એકાઉન્ટ કે જેને અનુસરવાની ફરજ પાડવામાં આવી છે, તે કોઈ નકલી બ્રાન્ડનું હોઈ શકે છે કે પછી કોઈ સેલિબ્રેટીનું ખોટું એકાઉન્ટ હોઈ શકે છે, જેનો ઉપયોગ ઉપરના ઉદાહરણની જેમ દુષિત માહિતી (Malicious Content) ફેલાવવા માટે ઉપયોગમાં લેવામાં આવી શકે.
- **માહિતી માટે :** કોઈનું સોશિયલ મીડિયા એકાઉન્ટ હેક કરવાનું એક કારણ તે વ્યક્તિ પાસેથી માહિતીની ચોરી કરવાનું પણ હોઈ શકે છે. પાસવર્ડ, બેંકો અથવા અન્ય ઓનલાઈન વ્યવહારોની વિગત, વ્યવસાય અંગેની વિગત, તમારી આદતો, ફોટો તથા મિત્રો સાથે કરેલી વાતચીત, ફરવા ગયેલા સ્થળોની વિગત વગેરે જેવી માહિતી હેકર્સ હેક કરેલ સોશિયલ મીડિયા એકાઉન્ટમાંથી ચોરી શકે છે.
- **છેતરપિંડી માટે :** હેકર ઘણીવાર કોઈ પ્રખ્યાત વ્યક્તિના એકાઉન્ટને કોમ્પ્રોમાઈઝ કરી તેમાંથી દાન માંગતી માહિતી મૂકે કે પછી કોઈ લોભામણી માહિતી આપે. આવી માહિતી જોઈ ઘણા લોકો મળેલી માહિતીની ખરાઈ કર્યા વગર અયોગ્ય નાણાકીય વ્યવહારો કરી છેતરાય છે.
- **કોઈને બદનામ કરવા માટે :** કોઈ પ્રતિભાશાળી કે નામાંકિત વ્યક્તિને બદનામ કરવા માટે પણ જે તે વ્યક્તિની પ્રોફાઈલ કોમ્પ્રોમાઈઝ કરવામાં આવે છે અને ત્યારબાદ તેના એકાઉન્ટનો ઉપયોગ અયોગ્ય સંદેશા મૂકવા માટે અથવા તો ખોટી અને ભ્રામક માહિતી મૂકવા માટે થાય છે. ટ્વિટરના ભૂતપૂર્વ CEO અને સોશિયલ મીડિયા પ્લેટફોર્મના સ્થાપક એવા ડોર્સીનું એકાઉન્ટ પણ હેક કરવામાં આવ્યું હતું, ત્યારબાદ હેકરે કોમ્પ્રોમાઈઝ થયેલા એકાઉન્ટ દ્વારા જાતિવાદ વિષયક અને અભદ્ર ટ્વીટ્સ પોસ્ટ કરવાનું ચાલુ કર્યું હતું.
- **નકલી સમાચાર ફેલાવવા માટે :** 23મી એપ્રિલ 2013ના રોજ, એસોસિએટેડ પ્રેસના ટ્વિટર એકાઉન્ટ સાથે ચેડા કરવામાં આવ્યા હતા. વ્હાઈટ હાઉસમાં વિસ્ફોટથી પ્રમુખ ઓબામાને ઈજા થઈ હોવાની ખોટી માહિતી આપવા માટે તે એકાઉન્ટનો દુરુપયોગ કરવામાં આવ્યો હતો. આ સંદેશની એક આડઅસર એ થઇ હતી કે ઉપરોકત માહિતી પોસ્ટ કર્યાની સેકંડોમાં જ તેનો ઉપયોગ ન્યૂયોર્ક સ્ટોક એકસચેન્જ પર ઓટોમેટેડ

ટ્રેડિંગ બોટ્સ દ્વારા નકારાત્મક ઘટનાઓના સંકેત તરીકે કરવામાં આવ્યો હતો જેને કારણે માર્કેટ ઇન્ડેક્સમાં નોંધપાત્ર ઘટાડો થયો હતો.

પ્રોફાઇલને કોમ્પ્રોમાઇઝ થતી બચાવવા માટે કેવા પગલાં લેશો

- તમામ સોશિયલ મીડિયા એકાઉન્ટમાં Two way Authentication રાખો.
- જે કોઈ તમને ઈ-મેઈલ અથવા ડાયરેક્ટ મેસેજ કરે છે તેને ક્યારેય તમારા સોશિયલ મીડિયા એકાઉન્ટની વિગત આપશો નહીં.
- ખૂબ સારી અને આકર્ષક ઑફર્સ અથવા શંકાસ્પદ સમાચાર ધરાવતા લેખો કે સંદેશો પર ક્યારેય ક્લિક કરશો નહીં, કારણ કે આવા પ્રકારના સંદેશાઓ ઘણીવાર દૂષિત એપ્લિકેશનો અથવા માલવેરનો શિકાર બનાવે છે.
- કોઈપણ અવાંછિત એપ્સને ક્યારેય ડાઉનલોડ કરશો નહીં, ખાસ કરીને જે તમારા વતી પોસ્ટ કરવાની પરવાનગી ધરાવે છે.
- કોઈપણ પરિસ્થિતિમાં પાસવર્ડનો પુનઃઉપયોગ ટાળો.
- તમારા પાસવર્ડ અને સુરક્ષા સેટિંગ્સ નિયમિતપણે અપડેટ કરો. મજબૂત પાસવર્ડનો ઉપયોગ કરો.
- જો તમે તમારા મિત્રનાં એકાઉન્ટમાંથી મુકાયેલી અયોગ્ય પોસ્ટ જુઓ છો તો સંભવ છે કે તેઓએ ખરેખર તે મોકલ્યું નથી. આવી પરિસ્થિતિમાં જો શક્ય હોય તો, તે વ્યક્તિનો એવી રીતે સંપર્ક કરો કે જેમાં સોશિયલ મીડિયા સામેલ ન હોય અને પૂછો કે શું તે ખરેખર તેમના તરફથી મોકલવામાં આવ્યું હતું. જો નહીં, તો તેમને ભલામણ કરો કે તેઓ તરત જ તેમનો પાસવર્ડ બદલી નાખે.
- તમે જાણતા ન હોય તેવા લોકોની Friend Request સ્વીકારવામાં સાવચેત રહો. આવી Friend Request સ્વીકારતા પહેલા હંમેશાં જરૂરી તપાસ કરવી.

5.7 દુષ્ટ સામગ્રી / માલિસિયસ કોન્ટેન્ટ (Malicious Content)

માલિસિયસ કોન્ટેન્ટ / દૂષિત સામગ્રી એ એવા પ્રકારની ડિજિટલ સામગ્રી (ફાઇલો, કોડ અથવા સ્ક્રિપ્ટ્સ) છે જેનો ઉપયોગ વ્યક્તિ, સંસ્થા, સિસ્ટમ અથવા નેટવર્કને નુકસાન પહોંચાડવા માટે થાય છે. દૂષિત સામગ્રી ઘણા સ્વરૂપે હોય શકે છે, નીચે તેના કેટલાક ઉદાહરણો આપેલા છે.

- **માલવેર :** માલવેર એ એક પ્રકારનું સોફ્ટવેર છે જે સિસ્ટમમાં ઘૂસણખોરી કરવા અને નુકસાન પહોંચાડવા અથવા માહિતીની ચોરી કરવા માટે રચાયેલ છે. સામાન્ય પ્રકારના માલવેરમાં વાયરસ, ટ્રોજન અને રેન્સમવેરનો સમાવેશ થાય છે.
- **ફિશિંગ ઇ-મેઇલ અથવા સંદેશાઓ :** ફિશિંગ ઇ-મેઇલ અથવા સંદેશાઓ વ્યક્તિઓને સંવેદનશીલ માહિતી, જેમ કે લૉગિન ઓળખપત્ર અથવા ક્રેડિટ કાર્ડ નંબર, અથવા માલવેર ડાઉનલોડ કરવા માટે છેતરવા માટે ડિઝાઇન કરવામાં આવ્યા છે.
- **દૂષિત સ્ક્રિપ્ટ્સ :** દૂષિત સ્ક્રિપ્ટો એ કોડ છે જે વેબસાઇટ્સ અથવા અન્ય ડિજિટલ સામગ્રીમાં એમ્બેડ કરવામાં આવે છે જેનો ઉપયોગ અનધિકૃત ક્રિયાઓ કરવા અથવા માહિતીની ચોરી કરવા માટે થઈ શકે છે.
- **દૂષિત ફાઇલો :** દૂષિત ફાઇલો, જેમ કે PDF અથવા એક્ઝિક્યુટેબલ ફાઇલો, સિસ્ટમમાં નબળાઈઓનો ઉપયોગ કરવા અથવા માલવેર ઇન્સ્ટોલ કરવા માટે ડિઝાઇન કરી શકાય છે.

- **એડવેર અને સ્પાયવેર :** એડવેર અને સ્પાયવેર એ એવા પ્રકારના સોફ્ટવેર છે જે વપરાશકર્તાની જાણ વગર સિસ્ટમ પર ઈન્સ્ટોલ કરી શકાય છે, અને તેનો ઉપયોગ માહિતી એકત્રિત કરવા અથવા અનિચ્છનીય જાહેરાતો પ્રદર્શિત કરવા માટે થઈ શકે છે.

દૂષિત સામગ્રી / માલિસિયસ કોન્ટેન્ટનાં લીધે થતા નુકસાન :

દૂષિત સામગ્રી વ્યક્તિ, સંસ્થા, સિસ્ટમ અથવા નેટવર્કને વિવિધ નુકસાન પહોંચાડી શકે છે, જેમાં નીચેનાનો સમાવેશ થાય છેઃ

- **સંવેદનશીલ માહિતીની ચોરી :** દૂષિત સામગ્રી સંવેદનશીલ માહિતી, જેમ કે પાસવર્ડ, ક્રેડિટ કાર્ડ નંબર અથવા અન્ય વ્યક્તિગત ડેટાની ચોરી કરવા માટે ડિઝાઈન કરી શકાય છે. આ માહિતીનો ઉપયોગ ઓળખની ચોરી અથવા અન્ય કપટપૂર્ણ પ્રવૃત્તિઓ માટે થઈ શકે છે.
- **સિસ્ટમ્સ અથવા નેટવર્ક્સને નુકસાન :** દૂષિત સામગ્રીને સિસ્ટમ્સ અથવા નેટવર્ક્સને નુકસાન પહોંચાડવા માટે ડિઝાઈન કરી શકાય છે, જેમ કે ફાઈલો કાઢી નાખવી, ફાઈલોને કરપ્ટ કરવી, સિસ્ટમ અને નેટવર્કની ગોઠવણીમાં ફેરફાર કરવો જેના લીધે સીસ્ટમ અથવા તો નેટવર્ક ક્રેશ થાય છે. વળી આનાથી ડેટા પણ ખોવાઈ શકે છે.
- **રેન્સમવેર હુમલાઓ :** રેન્સમવેર એ એક પ્રકારનો માલવેર છે જે પીડિતની ફાઈલોને એન્ક્રિપ્ટ કરી શકે છે અને ડિક્રિપ્શન કીના બદલામાં ચુકવણીની માંગ કરી શકે છે. આનાથી ડેટા ખોવાઈ શકે છે અથવા પીડિતને નાણાકીય નુકસાન થઈ શકે છે.
- **સિસ્ટમ્સ અથવા નેટવર્ક્સની અનધિકૃત ઍક્સેસ :** દૂષિત સામગ્રીનો ઉપયોગ સિસ્ટમ્સ અથવા નેટવર્ક્સની અનધિકૃત ઍક્સેસ મેળવવા માટે થઈ શકે છે, જેનાથી હુમલાખોરો માહિતી ચોરી શકે છે અથવા વધુ નુકસાન પહોંચાડે છે.
- **સેવાઓમાં વિક્ષેપ :** દૂષિત સામગ્રીનો ઉપયોગ ડિસ્ટ્રિબ્યુટેડ ડિનાયલ-ઓફ-સર્વિસ (DDoS) હુમલાઓ શરૂ કરવા માટે થઈ શકે છે, જે સિસ્ટમ તથા નેટવર્કનાં ટ્રાફિકને વધારી કાયદેસર વપરાશકર્તાઓ માટે અનુપલબ્ધ બનાવી શકે છે.
- **પ્રતિષ્ઠાને નુકસાન :** દૂષિત સામગ્રીનો ઉપયોગ વ્યક્તિઓ અથવા સંસ્થાઓ વિશે ખોટી અથવા નુકસાનકારક માહિતી ફેલાવવા માટે થઈ શકે છે, જે સંભવિત રીતે તેમની પ્રતિષ્ઠાને નુકસાન પહોંચાડે છે.

વિશ્વમાં કેટલાક મુખ્ય ઉદાહરણ :

- **રેન્સમવેર એટેક :** મે 2017 માં, WannaCry રેન્સમવેર હુમલાએ 150 દેશોમાં 200,000 થી વધુ કમ્પ્યૂટર્સને ચેપ લગાડ્યો હતો, જેના કારણે યુકેની નેશનલ હેલ્થ સર્વિસ (NHS) અને FedEx જેવી સંસ્થાઓમાં મોટા વિક્ષેપ પડ્યા હતા.
- **ફિશીંગ એટેક :** 2016 માં, ફિશિંગ હુમલાએ ડેમોક્રેટિક નેશનલ કમિટીને નિશાન બનાવ્યું હતું, જેના પરિણામે સંવેદનશીલ ઈમેલની ચોરી અને પ્રકાશન થયું હતું.
- **દૂષિત ફાઈલ ડાઉનલોડ :** 2019માં, ઝૂમ વિડિઓ કોન્ફરન્સિંગ સૉફ્ટવેરમાં એક નબળાઈ મળી આવી હતી જેણે હુમલાખોરોને વપરાશકર્તાઓને એક દૂષિત લિંક મોકલવાની મંજૂરી આપી હતી, જેને ક્લિક કરવામાં આવે ત્યારે, તેમના કમ્પ્યૂટર પર માલવેર ઈન્સ્ટોલ કરી શકે છે.
- **ઓળખપત્રની ચોરી :** 2020 માં, SolarWinds સપ્લાય ચેઈન એટેકમાં ઓળખપત્રની ચોરી કરવા અને યુએસ સરકાર અને માઈક્રોસોફ્ટ જેવી સંસ્થાઓની સંવેદનશીલ

માહિતીની ઍક્સેસ મેળવવા માટે માલવેરનો ઉપયોગ કરવામાં આવ્યો હતો.

આપણે આ સામે કેવી રીતે રક્ષણ મેળવી શકીએ ?

- લિંક્સ અથવા એટેચમેન્ટ પર કિલક કરવાનું ટાળો
- મજબૂત પાસવર્ડનો ઉપયોગ કરો
- તમારી ઓળખને સુરક્ષિત રાખો
- તમારા ડેટાનો બેકઅપ લો
- તમારી પાસે અદ્યતન એન્ટી વાઈરસ સોફ્ટવેર છે કે નહિ તેની ખાતરી કરો, જો ન હોય તો તે વહેલી તકે ઈન્સ્ટોલ કરો.
- તમારા બધા સૉફ્ટવેરને ઉપકરણો પર નવીનતમ સુરક્ષા પેચ સાથે અપ ટુ ડેટ રાખો
- તમે જે વેબસાઈટ પર છો તેની ચકાસણી કરો.
- માહિતી અપલોડ કરતાં પહેલાં ખાતરી કરો કે તે અન્ય લોકો સાથે શેર કરી શકાય તેવી છે કે કેમ.

5.8 ડિઝિટલ જોખમ (Digital Risk) ને ડિજિટલ સંરક્ષણ (Digital Defense)ની જરૂર

ડિજિટલ જોખમ એ કમ્પ્યૂટર, મોબાઈલ ઉપકરણો અથવા ઑનલાઈન સેવાઓ જેવી ડિજિટલ તકનીકોના ઉપયોગના પરિણામે નકારાત્મક અસરો અથવા નુકસાનની સંભવિતતાને દર્શાવે છે. આમાં ડેટા ગોપનીયતા, સાયબર સુરક્ષા, વ્યક્તિ તથા સંસ્થાની પ્રતિષ્ઠા જેવા જોખમો સામેલ હોઈ શકે છે.

ડિજિટલ જોખમોના કેટલાક ઉદાહરણો :

- **ડેટા ભંગ :** જ્યારે બિનઅધિકૃત વ્યક્તિઓ દ્વારા સંવેદનશીલ અથવા ગોપનીય માહિતી એક્સેસ કરવામાં આવે, ચોરવામાં આવે અથવા ખુલ્લી કરવામાં આવે ત્યારે ડેટાનો ભંગ થાય છે. આના પરિણામે નાણાકીય નુકસાન, પ્રતિષ્ઠાને નુકસાન અને કાનૂની પ્રશ્નો થઈ શકે છે.
- **સાયબર એટેક :** સાયબર એટેક એ દૂષિત હેતુઓ માટે કોમ્પ્યૂટર સિસ્ટમ અથવા નેટવર્કનો ભંગ કરવાનો ઈરાદાપૂર્વકનો પ્રયાસ છે, જેમ કે ડેટા ચોરી અથવા કામગીરીમાં વિક્ષેપ. સાયબર હુમલાના પરિણામે નાણાકીય નુકસાન તથા વ્યક્તિ કે સંસ્થાની પ્રતિષ્ઠાને નુકસાન થઈ શકે છે.
- **સોશિયલ મીડિયા જોખમો :** પ્રતિષ્ઠા, બ્રાન્ડ ઈમેજ અને ડેટા ગોપનીયતા સંબંધિત જોખમો સોશિયલ મીડિયા પ્લેટફોર્મ દ્વારા થઈ શકે છે. સોશિયલ મીડિયાનો ઉપયોગ ફિશિંગ હુમલાઓ અને સોશિયલ એન્જિનિયરિંગ કૌભાંડો માટે પણ થઈ શકે છે.
- **નિયમોનું પાલન ન કરી શકવાનું જોખમ :** ડેટા ગોપનીયતા, સાયબર સુરક્ષા અથવા અન્ય ડિજિટલ સમસ્યાઓ સંબંધિત કાનૂની અથવા નિયમનકારી આવશ્યકતાઓનું પાલન કરવામાં નિષ્ફળતા દંડ, કાનૂની દંડ અને પ્રતિષ્ઠાને નુકસાનમાં પરિણમી શકે છે.
- **તૃતીય-પક્ષ (Third Party) જોખમો :** ડિજિટલ ટેક્નોલૉજીમાં ઘણીવાર તૃતીય-પક્ષ (Third Party) વિક્રેતાઓ અથવા સેવા પ્રદાતાઓ સાથે કામ કરવાનો સમાવેશ થાય છે, જે ડેટા ગોપનીયતા, સુરક્ષા અને અનુપાલન (Complance) સંબંધિત જોખમો ઊભા શકે છે.

ડિજિટલ સંરક્ષણ (Digital Defense) :

ડિજિટલ સંરક્ષણમાં ડિજિટલ જોખમોને રોકવા અને સંભવિત જોખમો સામે રક્ષણ માટે સક્રિય પગલાં લેવાનો સમાવેશ થાય છે. સંગઠનો તેમના ડિજિટલ સંરક્ષણને મજબૂત કરવા માટે નીચે દર્શાવેલ કેટલાક પગલાં લઈ શકે છેઃ

- **જોખમ મૂલ્યાંકન કરો :** સંભવિત જોખમો અને નબળાઈઓને ઓળખવા માટે નિયમિતપણે ડિજિટલ જોખમોનું મૂલ્યાંકન કરો. આ સંસ્થાઓને, તેમના સંરક્ષણને પ્રાથમિકતા આપવામાં અને વધુ અસરકારક રીતે સંસાધનોની ફાળવણી કરવામાં મદદ કરી શકે છે.
- **સુરક્ષા નિયંત્રણો લાગુ કરો :** સાયબર ધમકીઓ સામે રક્ષણ આપવા માટે ફાયરવોલ, એન્ટીવાયરસ સોફ્ટવેર અને એક્સેસ કંટ્રોલ જેવા સુરક્ષા પગલાંનો અમલ કરો. સંક્રમણમાં અને બાકીના સમયે સંવેદનશીલ ડેટાને સુરક્ષિત રાખવા માટે એન્ક્રિપ્શનનો ઉપયોગ કરો.
- **કર્મચારીઓને શિક્ષિત કરો :** કર્મચારીઓને ડિજિટલ જોખમો અને ડેટા સુરક્ષા માટે શ્રેષ્ઠ પ્રયાસો અંગે નિયમિત તાલીમ આપો. કર્મચારીઓ ફિશિંગ સ્કેમ્સ, સોશિયલ એન્જિનિયરિંગ હુમલાઓ અને અન્ય સાયબર ધમકીઓ જેવા સંભવિત જોખમોથી વાકેફ હોવા જોઈએ.
- **નેટવર્ક્સ અને સિસ્ટમ્સનું નિરીક્ષણ કરો :** સંભવિત જોખમોના સંકેતો માટે નિયમિતપણે નેટવકર્સ અને સિસ્ટમ્સનું નિરીક્ષણ કરો. આ સંભિવત સાયબર હુમલાઓ અથવા ડેટા ભંગને નોંધપાત્ર નુકસાન પહોંચાડે તે પહેલાં તેને ઓળખવામાં અને તેનો પ્રતિસાદ આપવામાં મદદ કરી શકે છે.
- **ઘટના પ્રતિભાવ યોજનાઓ (Incident Response Plans) વિકસાવો :** ડેટા ભંગ અથવા સાયબર હુમલા જેવી સુરક્ષા ઘટનાઓનો પ્રતિસાદ આપવા માટે એક યોજના વિકસાવો. આમાં વપરાશકર્તાઓને સૂચિત કરવા, પુરાવા સાચવવા અને સિસ્ટમ્સ અને ડેટાને પુનઃસ્થાપિત કરવા માટેની પ્રક્રિયાઓનો સમાવેશ થવો જોઈએ.
- **સૉફ્ટવેરને અદ્યતન રાખો :** ખાતરી કરો કે બધા સૉફ્ટવેર અને હાર્ડવેર નવીનતમ સુરક્ષા પેચ અને અપડેટ્સ સાથે અદ્યતન હોય. આનાથી હુમલાખોરોને નબળાઈઓ ગોતવી અઘરી બની શકે છે.

આ પગલાંનો અમલ કરીને અને ડિજિટલ સંરક્ષણ માટે સક્રિય અભિગમ અપનાવીને, સંસ્થાઓ ડિજિટલ જોખમો સામે પોતાને વધુ સારી રીતે સુરક્ષિત કરી શકે છે અને ડિજિટલ તકનીકોના ઉપયોગથી સંબંધિત નકારાત્મક પરિણામોની સંભાવનાને ઘટાડી શકે છે.

- **સારાંશ**

આ પ્રકરણમાં સાયબર ગુનાની બહુપક્ષીય પ્રકૃતિ અને મજબૂત સાયબર સુરક્ષા પગલાંની અનિવાર્ય જરૂરિયાતનું ઊંડાણપૂર્વકનું સંશોધનની માહિતી પ્રાપ્ત કરી. NHS સાયબર હુમલો, Crabanak હુમલો, Yahoo ડેટા ભંગ અને સાયબર અપરાધ દ્વારા નાણાકીય છેતરપિંડી જેવી નોંધપાત્ર ઘટનાઓને હાઈલાઈટ કરીને, આ ઘટનાઓમાંથી શીખેલા વાસ્તવિક-વિશ્વની અસરો જોઈ શકાય છે.

2017માં WannaCry રેન્સમવેરના કારણે થયેલા NHS સાયબર હુમલાએ જટિલ ઈન્ફ્રાસ્ટ્રક્ચરમાં સાયબર નબળાઈઓના વિનાશક પરિણામો દર્શાવ્યા હતા. આ ઘટનાએ સમયસર સોફ્ટવેર અપડેટ્સ અને મહત્ત્વપૂર્ણ સેવાઓને વિક્ષેપજનક હુમલાઓથી બચાવવા

માટે આકસ્મિક આયોજનના મહત્ત્વ દર્શાવ્યા છે.

Carbanak એટેક, નાણાકીય સંસ્થાઓને નિશાન બનાવતા એક અત્યાધુનિક સાયબર હેસ્ટ, સાયબર ગુનેગારોની વધતી જતી જટિલતા અને હિંમતને જાહેર કરે છે. નબળાઈઓનો ઉપયોગ કરીને અને અદ્યતન યુક્તિઓનો ઉપયોગ કરીને, Carbanak જૂથે વિશ્વભરની બેંકોમાંથી સફળતાપૂર્વક એક અબજ ડૉલરની ચોરી કરી. આ કેસ નાણાકી.ય ક્ષેત્રની અંદર સુરક્ષા પ્રોટોકોલ્સ અને સતત દેખરેખની જરૂરિયાતને પ્રકાશિત કરે છે. ફિશિંગ, ઓળખની ચોરી અને ઓનલાઈન કૌભાંડો સહિત સાયબર અપરાધ દ્વારા નાણાકીય છેતરપિંડી એક વ્યાપક ખતરો છે. આ ગુનાઓ નાણાકીય પ્રવૃત્તિઓ માટે ડિજિટલ વ્યવહારો અને ઇન્ટરનેટ પરની વધતી જતી નિર્ભરતાનું શોષણ કરે છે, ગ્રાહકો અને વ્યવસાયોને સુરક્ષિત રાખવા માટે ઉચ્ચ જાગૃતિ, સુરક્ષિત પ્રમાણીકરણ પદ્ધતિઓ અને નિયમનકારી માળખાની જરૂરિયાત પર ભાર મૂકે છે. જેમ જેમ ટેક્નોલોજી આગળ વધી રહી છે તેમ, સાયબર સુરક્ષા માટે સક્રિય, બહુ-સ્તરીય અભિગમ, શિક્ષણ અને સહયોગ સાથે, આપણા ડિજિટલ વિશ્વને સુરક્ષિત કરવા માટે આવશ્ક બનશે.

5.9 તમારી પ્રગતિ ચકાસો.

1. શા માટે હેકર્સ સોશિયલ મીડિયા પ્રોફાઈલ સમાધાન (Profile Compromise) કરે છે ?

___

2. આપણે ફિશિંગનો ભોગ ન બનીએ તેના માટે કેવી તકેદારી રાખવી ?

___

3. સોશિયલ એન્જિનિયરિંગ પ્રકારના હુમલા સામે રક્ષણ મેળવવા કેવી તકેદારી રાખવી ?

___

4. સ્કેમર્સ તથા કેટફિશર્સ વચ્ચેનો તફાવત જણાવો.

___

5. દૂષિત સામગ્રી/માલિસિયસ કોન્ટેન્ટનાં લીધે થતા નુકસાન સામે કેવી રીતે બચી શકાય ?

___

5.10 ચાવીરૂપ શબ્દો

- **રેન્સમવેર** - એક પ્રકારનું સોફ્ટવેર જે કમ્પ્યૂટર, મોબાઈને હેક કરે છે અને નાણાની માંગણી કરે છે.
- **ડેટા બ્રીચ** - સંગ્રહ કરેલા ડેટાને ચોરીથી ઉઠાંતરી કરવી.

5.9 સંદર્ભસૂચિ

1. Abelson, R. & Goldstein, M. Millions of Anthem customers targeted in cyberattack.
2. English junior doctors in 2016. BMJ Open 8, e019319 (2018).
3. Furnivall, D., Bottle, A. & Aylin, P. Retrospective analysis of the national impact of industrial action by
4. Gomez, J. & Konschak, C. Cyber-security in healthcare-understanding the new world threat.
5. https://www.divurgent.com/wp-content/uploads/2015/03/Cyber-Security-Healthcarepdf.pdf (2015).
6. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-WannaCry-
7. https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html(2015).
8. McDonald, C. Computerization can create safety hazards: a bar-coding near miss. Ann. Intern. Med. 144,510 (2016).
9. McGee, M. A new in-depth analysis of Anthem breach. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 (2017).
10. National Audit Office. Investigation: WannaCry cyber-attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (2017).
11. ransomware-cyber-attack-cio-review.pdf (2018).
12. Smart, W. Lessons learned review of the WannaCry ransomware cyber-attack.

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-93-5598-630-6